CSPP-OS - COTS Security Protection Profile - Operating Systems

(formerly: CS2-OS - Protection Profile for Near-Term COTS Operating Systems)

DRAFT VERSION 0.3

by Gary Stoneburner (NIST)

Date - 4/4/00

Revision History

Version 0.3, date 12/9/99, name change to reflect CS2 to CSPP change, incorporate editorial changes made in released version of CSPP, and deletion of requirement for trusted path with modification to related objective (not a part of most COTS OSs).

Version 0.2, date 7/27/99, editorial changes, completed TBDs in functional components, and added functional requirements for IT-environment.

Version 0.1, initial version, 3/25/99 - some TBDs (operations on functional components and functional requirements details for the IT-environment).

DRAFT, SUBJECT to CHANGE

NIST United States Department of Commerce
National Institute of Standards and Technology

TABLE OF CONTENTS

SECTION PAGE

TABLE OF TABLES

TABLE **PAGE**

1. INTRODUCTION

1.1 IDENTIFICATION

Title: CSPP-OS - COTS Security Protection Profile - Operating Systems
(formerly: CS2-OS – PP for Near-Term COTS Operating Systems)

Assurance level: EAL2 – augmented (EAL-CSPP)

Registration: <To be filled in upon registration>

Keywords: Protection Profile, COTS, general-purpose operating systems, networked information systems, baseline protection

1.2 OVERVIEW

Purpose

The purpose of CSPP-OS is to define, and specify the requirements necessary to solve, the security problem that COTS operating systems (perhaps with add-on packages) can be expected to address in the near-term.

This PP is developed using the guidance from [CSPP].

Scope

Type of system. CSPP-OS provides the requirements necessary to specify needs for operating systems in both stand-alone and distributed, multi-user information systems.

Type of access. CSPP-OS recognizes two forms of legitimate access; namely, public access and "authenticated users". With public access, the user does not have a unique identifier and is not authenticated prior to access. An example is access to information on a publicly accessible web page. Such users have legitimate access, but are differentiated from "authenticated users" who are (1) uniquely identifiable by the system, (2) have legitimate access beyond publicly available information, and (3) are authenticated prior to being granted such access.

Nature of use. CSPP-OS compliant operating systems are suitable for the protection of information in real-world environments, both commercial and government.

- Within government environments, CSPP-OS compliant OSs are considered to be suitable for specifying the baseline protection requirements for sensitive-but-unclassified or single level classified information in an environment where all authenticated users are cleared for the level of information being processed. For classified environments, public access is not allowed into a CSPP-OS compliant OS. For sensitive-but unclassified environments, public access may be acceptable with additional controls, beyond OS mechanisms, supplied by the operational environment.

- For commercial environments, CSPP-OS compliant OSs are suitable for specifying the baseline protection requirements for information in environments where all authenticated users are either (1) trusted to not maliciously attempt to circumvent nor by-pass access controls or (2) lack the motivation or capability for sophisticated penetration attempts. Public access is allowed with environmental controls over and beyond the OS supplied security mechanisms.

Key Assumptions. Key assumptions that apply for CSPP-OS compliant OSs are –

- the Target of Evaluation (TOE, the OS for which requirements are being specified) is comprised of near-term, commercial off the shelf (COTS) information technology
- authenticated users recognize the need for a secure IT environment
- authenticated users can be reasonably trusted to correctly apply the organization's security policies in their discretionary actions
- competent security administration is performed
- business/mission process automation is implemented with due regard for what can not be expected of a CSPP-OS compliant OS.

Summary of CSPP-OS Requirements

Systems incorporating main-stream, COTS operating systems (OSs) achieve the advantages such products offer; for example, high-functionality with low-cost. However, these advantages are not achieved without some tradeoffs; an example of which is security capability. CSPP-OS identifies a cost-effective, security baseline for systems built from COTS OSs, ensuring that reasonable security expectations are achieved.

CSPP-OS also identifies those areas where it is not realistic to expect a typical COTS operating system to provide sufficient protection. These areas are the direct result of the fact that the driving factors for COTS (functionality, cost, and time to market) have tended to work against increasing the security capabilities beyond those identified in CSPP-OS.

Assurance. CSPP-OS assurances have been selected to provide the level of confidence resulting from (1) existing best practices for COTS development and (2) no extensive (and hence costly) third-party evaluation. This equates, in summary, to OS technical countermeasures that -

- are sufficient for controlling a community of benign (i.e., not intentionally malicious) authenticated users
- can provide protection against unsophisticated, technical attacks
- can not be expected to provide sufficient protection against sophisticated, technical attacks (to include denial-of-service)

Functionality. The CSPP-OS operating system addresses these user needs -

- enforcing an access control policy between active entities (subjects) and passive objects based on subject identity and allowed actions
- providing support for controlling access based upon environmental constraints such as time-of-day and port-of-entry
- resistance to resource depletion by providing resource allocation features
- providing mechanisms to detect some insecurities
- providing mechanisms for trusted recovery in the event of some system failures or detected insecurities
- supporting these capabilities in a distributed system connected via an untrusted network

CSPP-OS compliant OSs are not expected to –

- provide the label-based controls appropriate for protecting controlled information (such as government classified, company proprietary, or export restricted data) in environments containing authenticated users who are not allowed access to such information
- protect against malicious abuse of authorized privileges
- adequately protect against sophisticated attacks (to include denial of service)
- provide sufficient protection against installation, operation, or administration errors

2. TOE DESCRIPTION

The Target of Evaluation (TOE) in a common criteria protection profile is the information technology component or system for which requirements are to be specified. This section, TOE Description, describes the CSPP-OS in terms of the targets of evaluation (TOEs) covered. These TOEs are identified by class of product, the operational environment, and the required security functionality.

2.1 PRODUCT CLASS

CSPP-OS covers general-purpose operating systems in both stand-alone and networked environments. The TOEs covered by this PP permit one or more processors and attached peripheral and storage devices to be used by multiple users to perform a variety of functions requiring controlled, shared access to processing capability and information.

The TOE will provide user services directly or serve as a platform for networked applications.

The TOE will support protected communications across an untrusted network.

The TOE may consist of a standard operating system with add-on packages to increase the base functionality.

2.2 OPERATIONAL ENVIRONMENT

The TOE supports the active entities of human users and software processes. Human users, in conjunction with system processes, are accountable for all system activities. The TOE generates processes that act on behalf of either a specific human user or a uniquely identifiable system process. A process requests and consumes resources on behalf of its unique, associated user or system process. In a networked environment, a process may invoke another process on a different system.

The TOE is intended for use in a networked environment and will support one or more types of communication and protocols, such as:

- Synchronous process communication; e.g., remote procedure calls (RPC)
- Asynchronous process communication; e.g., message passing using user datagram protocol (UDP)
- Network management protocols; e.g., simple network management protocol (SNMP)

A compliant TOE will support –

- Users with networked access to the TOE across an untrusted network (that is, mechanisms operating within the TOE cooperate with mechanisms in other components to securely exchange information across an untrusted network)
- Several users executing tasks on the same system concurrently
- Sharing resources, such as printer and mass storage, across a network

2.3 REQUIRED SECURITY FUNCTIONALITY

CSPP-OS specifies the requirements for an operating system with the security functionality listed below.

- Executing the access control policy of the imposed IT security policy
- Assigning a unique identifier to each authenticated user
- Assigning a unique identifier to each system process, including those not running on behalf of a human user (e.g., processes started at system bootup like the Unix "inetd")
- Authenticating the claimed user identity before allowing any user to perform any actions other than a well-defined set of operations (e.g., reading from a public web site)
- Auditing in support of individual accountability and detection of and response to insecurity
- Enabling access authorization management; i.e., the initialization, assignment, and modification of access rights (e.g. read, write, execute) to data objects with respect to (1) active entity name or group membership and (2) environmental constraints such as time-of-day and port-of-entry.
- Resource allocation features providing a measure of resistance to resource depletion
- Mechanisms for detecting some insecurities
- System recovery features providing a measure of survivability in the face of system failures and insecurities
- Automated support to help in the verification of secure delivery, installation, operation, and administration

3. SECURITY ENVIRONMENT

3.1 INTRODUCTION

This section identifies the following:

- significant assumptions about the operational environment for CSPP-OS compliant OSs
- organizational security policies for which CSPP-OS compliant OSs are appropriate
- IT-related threats to the organization countered by the information technology in the notional information system of which compliant OSs are a part
- threats requiring either reliance on environmental controls to provide sufficient protection or explicit risk acceptance
- general description of the assurance required for CSPP-OS

By providing the information describe above, this section gives the basis for the security objectives described in section 4 and hence the specific security requirements listed in sections 5 and 6.

3.2 SECURE USAGE ASSUMPTIONS

The specific conditions listed below are key assumptions. These assumptions include both practical realities considered in the development of security requirements for CSPP-OS compliant OSs and essential environmental constraints on the use of compliant TOEs.

Table 3.2-1 – Security assumptions - TOE

Name	Assumption	Discussion
A.COTS	The TOE is constructed from near-term achievable, commercial off the shelf information technology.	This assumption is a key driver in determining the nature of the expectations toward, and hence the requirements to placed upon, the TOE.
A.MALICIOUS-INSIDER	The TOE is not expected to be able to sufficiently mitigate the risks resulting from malicious abuse of authorized privileges.	It is not reasonable to expect near-term COTS products to provide sufficient protection against the malicious actions of authorized individuals.
A.NO-LABELS	The TOE does not have to provide label-based access controls.	It is an assumption, based upon currently available technology and current common practice, that label based access controls will not be included in near-term COTS.
A.SOPHISTICATED-ATTACK	The TOE is not expected to be able to sufficiently mitigate risks resulting from application of sophisticated attack methods.	It is not reasonable to expect near-term achievable COTS to be able to resist sophisticated attacks.

Table 3.2-2 – Security assumptions - Personnel

Name	Assumption	Discussion
A. ADMIN	The security features of the TOE are competently administered on an on-going basis.	It is essential that security administration be both competent and on-going.
A.USER-NEED	Authenticated users recognize the need for a secure IT environment.	It is essential that the authenticated users appreciate the need for security. Otherwise they are likely to try and circumvent it.
A.USER-TRUST	Authenticated users are generally trusted to perform discretionary actions in accordance with security policies.	Authenticated users will have a fair amount of discretion with CSPP-OS systems and must therefore be trusted. However, this “trust” is not absolute, and hence the phrase “generally trusted”.

3.3 ORGANIZATIONAL SECURITY POLICIES

The organizational security policies discussed below are addressed by the notional system containing CSPP-OS compliant OSs.

Table 3.3-1 – Security policies

Name	**Policy**	**Discussion**
P.ACCESS	Access rights to specific data objects are determined by object attributes assigned to that object, user identity, user attributes, and environmental conditions as defined by the security policy.	CSPP-OS supports organizational policies which grant or deny access to objects using rules driven by attributes of the user (such as user identity, group, etc.), attributes of the object (such as permission bits), type of access (such as read or write), and environmental conditions (such as time-of-day).
P.ACCOUNT	Users must be held accountable for security-relevant actions.	CSPP-OS supports organizational policies requiring that users are held accountable for their actions, facilitating after-the-fact investigations and providing some deterrence to improper actions.
P.COMPLY	The implementation and use of the organization's IT systems must comply with all applicable laws, regulations, and contractual agreements imposed on the organization.	The organization will meet all requirements imposed upon it from the outside; for example: government regulations, national and local laws, and contractual agreements.
P.DUE-CARE	The organization's IT systems must be implemented and operated in a manner that represents due care and diligence with respect to risks to the organization.	It is important that the level of security afforded the IT system be in accordance with what is generally considered adequate within the business or government sector in which the organization is placed.
P.INFO-FLOW	Information flow between IT components must be in accordance with established information flow policies.	CSPP includes information flow control as this is needed in many environments. While this might not be implemented by mechanisms within the CSPP-OS TOE, the IT system, of which the TOE is a part, will likely have to meet this policy.
P.KNOWN	Except for a well-defined set of allowed operations, users of the TOE must be identified and authenticated before TOE access can be granted.	Beyond a well-defined set of actions such as read access to a public web-server, there is a finite community of known, authenticated users who are authenticated before being allowed access.
P.NETWORK	The organization's IT security policy must be maintained in the environment of distributed systems interconnected via insecure networking.	Since CSPP-OS systems will likely be interconnected across untrusted networking, this policy statement will have a significant impact on CSPP-OS requirement definition.

Name	Policy	Discussion
P.PHYSICAL	The processing resources of the TOE that must be physically protected in order to ensure that security objectives are met will be located within controlled access facilities that mitigate unauthorized, physical access.	A TOE will not be able to meet its security requirements unless at least a minimum degree of physical security is provided.
P.SURVIVE	The IT system, in conjunction with its environment, must be resilient to insecurity, resisting the insecurity and/or providing the means to detect an insecurity and recover from it.	CSPP-OS systems will provide a measure of this resilience through functionality and assurances that resist, detect, and recover from insecurities. For sophisticated attacks, a large portion of this resilience is provided by the TOE environment.
P.TRAINING	Authenticated users of the system must be adequately trained, enabling them to (1) effectively implement organizational security policies with respect to their discretionary actions and (2) support the need for non-discretionary controls implemented to enforce these policies.	Once granted legitimate access, authenticated users are expected to use IT resources and information only in accordance with the organizational security policy. In order for this to be possible, these users must be adequately trained both to understand the purpose and need for security controls and to be able to make secure decisions with respect to their discretionary actions.
P.USAGE	The organization’s IT resources must be used for only for authorized purposes.	CSPP-OS systems must, in conjunction with its environment, ensure that the organization’s information technology is not used for unauthorized purposes.

3.4 THREATS TO SECURITY

The technical countermeasures of systems comprised of near-term COTS are required to counter threats which may be broadly categorized as -

- the threat of unsophisticated, malicious attacks from individuals other than authenticated users
- the threat of authenticated users attempting, non-maliciously to gain unauthorized access or to perform an unauthorized operation. Such attempts may be performed to “get the job done”, out of curiosity, as a challenge, or as a result of an error.

Other threats that can affect system security must be dealt with in conjunction with controls provided by the operating environment or risk accepted.

The threats facing near-term COTS systems, and CSPP-OS compliant OSs in particular, are listed in Tables 3.4-1 through 3.4-3 and discussed further in sections 3.4.1 through 3.4.3 as follows:

Table 3.4-1 and section 3.4.1: Threats addressed by the environment

Table 3.4-2 and section 3.4.2: Threats addressed by the TOE

Table 3.4-3 and section 3.4.3: Threats addressed jointly by the TOE and its environment

Table 3.4-1 – Security threats addressed by TOE's Environment

T.ACCESS-NON-TECHNICAL	An authenticated user may gain non-malicious, unauthorized access using non-technical means.
T.ACCESS-Non-TOE	An authenticated user may gain unauthorized, non-malicious access to a resource or to information not directly controlled by the TOE via user error, system error, or an unsophisticated, technical attack.
T.AUDIT-CONFIDENTIALITY-Non-TOE	For audit trails not under control of the TOE, records of security events may be disclosed to unauthorized individuals or processes.
T.AUDIT-CORRUPTED-Non-TOE	For audit trails not under control of the TOE, records of security events may be subjected to unauthorized modification or destruction.
T.DENIAL-Non-TOE	The IT (other than the TOE) may be subjected to an unsophisticated, denial-of-service attack.
T.DENIAL-SOPHISTICATED	The system may be subjected to a sophisticated, denial-of-service attack.
T.ENTRY-NON-TECHNICAL	An individual, other than an authenticated user, may gain access to processing resources or information using non-technical means.
T.ENTRY-Non-TOE	An individual other than an authenticated user may gain unauthorized, malicious access to processing resources or information not controlled by the TOE via an unsophisticated, technical attack.
T.ENTRY-SOPHISTICATED	An individual, other than an authenticated user, may gain access to processing resources or information using a sophisticated, technical attack.
T.OBSERVE-Non-TOE	Events occur in operation of IT (other than the TOE) that compromise IT security; but that IT, due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.
T.PHYSICAL	Security-critical parts of the system may be subjected to a physical attack that may compromise security.
T.RECORD-EVENT-Non-TOE	Security relevant events not under control of the TOE may not be recorded.
T.TRACEABLE-Non-TOE	Security relevant events not under control of the TOE may not be traceable to the user or system process associated with the event.

Table 3.4-2 – Security threats addressed by TOE

Name	Threat
T.ACCESS-TOE	An authenticated user may gain unauthorized, non-malicious access to the TOE, or a resource or to information directly controlled by the TOE via user error, system error, or an unsophisticated, technical attack.
T.AUDIT-CONFIDENTIALITY-TOE	For audit trails under control of the TOE, records of security events may be disclosed to unauthorized individuals or processes.
T.AUDIT-CORRUPTED-TOE	For audit trails under control of the TOE, records of security events may be subjected to unauthorized modification or destruction.
T.CRASH-TOE	The secure state of the TOE could be compromised in the event of a system crash.
T.DENIAL-TOE	The TOE may be subjected to an unsophisticated, denial-of-service attack.
T.ENTRY-TOE	An individual other than an authenticated user may gain unauthorized, malicious access to TOE controlled processing resources or information via an unsophisticated, technical attack.
T.OBSERVE-TOE	Events occur in TOE operation that compromise IT security but the TOE , due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.
T.RECORD-EVENT-TOE	Security relevant events controlled by the TOE may not be recorded.
T.RESOURCES	The shared, internal TOE resources may become exhausted due to system error or non-malicious user actions.
T.TOE-CORRUPTED	The security state of the TOE, as a result of a lower-grade attack, may be intentionally corrupted to enable future insecurities.
T.TRACEABLE-TOE	Security relevant events controlled by the TOE may not be traceable to the user or system process associated with the event.

Table 3.4-3 – Security threats addressed Jointly by TOE and Environment

T.ACCESS-MALICIOUS	An authenticated user may obtain unauthorized access for malicious purposes.
T.ADMIN-ERROR	The security of the system may be reduced or defeated due to errors or omissions in the administration of the security features of the system.
T.CRASH-SYSTEM	The secure state of the system could be compromised in the event of a system crash.
T.INSTALL	The system may be delivered or installed in a manner that undermines security.
T.OPERATE	Security failures may occur because of improper operation of the system; e.g., the abuse of authorized privileges.
T.SYSTEM-CORRUPTED	The security state of the system, as a result of another threat, may be intentionally corrupted to enable future insecurities.

3.4.1 Threats environment addresses

The threats discussed below must be countered but are not addressed by the technical countermeasures within the CSPP-OS compliant TOE. Such threats must therefore, be addressed by the operating environment. Note that a measure of explicit risk acceptance is frequently a viable option.

T.ACCESS-NON-TECHNICAL: An authenticated user may gain non-malicious, unauthorized access using non-technical means.

The use of non-technical attack means; for example, social engineering or dumpster diving; is beyond the scope of TOE protections and must be addressed by the environment.

T.ACCESS-Non-TOE: An authenticated user may gain unauthorized, non-malicious access to a resource or to information not controlled by the TOE via user error, system error, or an unsophisticated, technical attack.

An authenticated user is someone who is (1) uniquely identifiable by the system, (2) has legitimate access beyond publicly available information, and (3) is authenticated prior to being granted such access.

By virtue of having access, the threat posed from authenticated users is inherently greater than that posed from unauthorized individuals. CSPP systems are expected to have only the assurances necessary to cover the threat of non-malicious actions by authenticated users; i.e., sufficient confidence in light of the fact that only non-malicious actions are covered.

There are two broad categories of users with respect to this threat:

- The first category are persons who possess little technical skills, do not have access to sophisticated attack tools, they have some rights of access, and are mostly trusted not to attempt to maliciously subvert the system nor maliciously exploit the information stored thereon. Users in this category may be motivated by curiosity to gain access to information for which they have no authorization.

- The second category of users is technically skilled or has access to sophisticated attack tools and some may attempt to bypass system controls as a technical challenge or as a result of curiosity. CSPP compliant components and systems would generally be used in environments where these users are highly trusted not to attempt to maliciously subvert the system nor to maliciously exploit the information stored thereon.

T.AUDIT-CONFIDENTIALITY-Non-TOE: Records of security events not under control of the TOE may be disclosed to unauthorized individuals or processes.

System security depends in part on the ability of the system to detect and report the occurrence of security relevant events, to determine the identity of those responsible for such events, and to protect the event records from unauthorized access, modification, or destruction.

T.AUDIT-CORRUPTED-Non-TOE: Records of security events not under control of the TOE may be subjected to unauthorized modification or destruction.

T.DENIAL-Non-TOE: The IT other than the TOE may be subjected to an unsophisticated, denial-of-service attack.

The IT in the TOE environment is expected to be able to withstand unsophisticated denial-of-service attacks.

T.DENIAL-SOPHISTICATED: The system may be subjected to a sophisticated, denial-of-service attack.

A system built from near-term COTS is not expected to be capable of resisting sophisticated attacks. Therefore, such a system must rely on protections provided by its non-IT environment to maintain availability in the face of such threats.

T.ENTRY-NON-TECHNICAL: An individual, other than an authenticated user, may gain access to processing resources or information using non-technical means.

T.ENTRY-Non-TOE: An individual other than an authenticated user may gain unauthorized, malicious access to processing resources or information not controlled by the TOE via an unsophisticated, technical attack.

The mechanisms and assurances of a near-term COTS system will resist low-grade technical attacks. (Resistance to higher-grade attacks, when such resistance is required, must be provide by the system’s operational environment.)

T.ENTRY-SOPHISTICATED: An individual, other than an authenticated user, may gain access to processing resources or information using a sophisticated, technical attack.

A system built from near-term COTS is not expected to protect itself against sophisticated, technical attacks. Therefore, this threat is largely addressed by the system’s operational environment.

T.OBSERVE-Non-TOE: Events occur in operation of IT other than the TOE that compromise security but the IT, due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.

This is the threat of an administrator or user not detecting a security problem because of errors or omissions in the IT’s human interface. The IT is then used in a manner which is insecure but which the administrator or user reasonably, but incorrectly, believes to be secure.

T.PHYSICAL: Security-critical parts of the system may be subjected to a physical attack that may compromise security.

The security offered by CSPP can be assured only to the extent that the hardware and software relied upon to enforce the security policy is physically protected from unauthorized physical modification and from technical attacks at the hardware level. Examples of such attacks are using electromagnetic pulse weapons, intercepting radiated electronic emissions, and passive monitoring or active attacking of physical transmission medium (e.g., coax, twisted-pair, or fiber optic cable).

T.RECORD-EVENT-Non-TOE: Security relevant events which IT other than the TOE is expected to record may not be recorded.

T.TRACEABLE-Non-TOE: Due to the IT other than the TOE, security relevant events may not be traceable to the user or system process associated with the event.

3.4.2 Threats TOE addresses

Technical countermeasures within the CSPP-OS compliant TOE address the threats discussed below.

T.ACCESS-TOE: An authenticated user may gain unauthorized, non-malicious access to a resource or to information controlled by the TOE via user error, system error, or an unsophisticated, technical attack.

An authenticated user is someone who is (1) uniquely identifiable by the system, (2) has legitimate access beyond publicly available information, and (3) is authenticated prior to being granted such access.

By virtue of having access, the threat posed from authenticated users is inherently greater than that posed from unauthorized individuals. CSPP-OS operating systems are required to have only the assurances necessary to cover the threat of non-malicious actions by authenticated users; i.e., sufficient confidence in light of the fact that only non-malicious actions are covered.

There are two broad categories of users with respect to this threat:

- The first category are persons who possess little technical skills, do not have access to sophisticated attack tools, and, because they have some rights of access, are mostly trusted not to attempt to maliciously subvert the system nor maliciously exploit the information stored thereon. Users in this category may be motivated by curiosity to gain access to information for which they have no authorization.

- The second category of users is technically skilled or has access to sophisticated attack tools and some may attempt to bypass system controls as a technical challenge or as a result of curiosity. CSPP-OS compliant operating systems would generally be used in environments where these users are highly trusted not to attempt to maliciously subvert the system nor to maliciously exploit the information stored thereon.

T.AUDIT-CONFIDENTIALITY-TOE: Records of security events under control of the TOE may be disclosed to unauthorized individuals or processes.

TOE security depends in part on the ability of the TOE to detect and report the occurrence of security relevant events, to determine the identity of those responsible for such events, and to protect the event records from unauthorized access, modification, or destruction.

T.AUDIT-CORRUPTED-TOE: Records of security events under control of the TOE may be subjected to unauthorized modification or destruction.

T.CRASH-TOE: The secure state of the TOE could be compromised in the event of a system crash.

For the TOE to protect the information it controls, it must remain in a secure state, including after recovery from a system failure or discontinuity of service.

System crash can occur with inadequate mechanisms for secure recovery. Data objects and audit information may be modified or lost and system software may be corrupted.

T.DENIAL-TOE: The TOE may be subjected to an unsophisticated, denial-of-service attack.

The TOE must be able to withstand unsophisticated denial-of-service attacks.

T.ENTRY-TOE: An individual other than an authenticated user may gain unauthorized, malicious access to processing resources or information controlled by the TOE via an unsophisticated, technical attack.

The mechanisms and assurances of a TOE compliant with this PP will resist low-grade technical attacks. (Resistance to higher-grade attacks, when such resistance is required, must be provide by the TOE operational environment.)

T.OBSERVE-TOE: Events occur in TOE operation that compromise IT security but the TOE, due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.

This is the threat of an administrator or user not detecting a security problem because of errors or omissions in the TOE's human interface. The TOE is then used in a manner which is insecure but which the administrator or user reasonably, but incorrectly, believes to be secure.

T.RECORD-EVENT-TOE: Security relevant events which the TOE is expected to record may not be recorded.

T.RESOURCES: The shared, internal TOE resources may become exhausted due to system error or non-malicious user actions.

System availability depends partly on the availability of shared resources.

T.TOE-CORRUPTED: The security state of the TOE, as a result of a lower-grade attack, may be intentionally corrupted to enable future insecurities.

System security depends to a large degree on the integrity of the hardware and software implementing the security functionality. If this is intentionally corrupted, the TOE will be unable to maintain a secure state.

T.TRACEABLE-TOE: Due to the TOE, security relevant events may not be traceable to the user or system process associated with the event.

3.4.3 Threats TOE and Environment jointly address

These threats are addressed by a combination of technical controls within the TOE and environmental controls (both technical and non-technical).

T.ACCESS-MALICIOUS: An authenticated user may obtain unauthorized access for malicious purposes.

CSPP-OS functionality and assurances are sufficient mitigation for non-malicious actions by authenticated users. The greater risk from malicious actions by authenticated users must be addressed in conjunction with the environment.

T.ADMIN-ERROR: The system security may be reduced or defeated due to errors or omissions in the administration of the security features of the TOE or other IT.

Authenticated users or external threat agents may, through accidental discovery or directed search, discover inadequacies in the security administration of the TOE, or other IT, which permit them to gain unauthorized access.

T.CRASH-SYSTEM: The secure state of the system could be compromised in the event of a system crash.

For the IT to protect the information it controls, it must remain in a secure state, including after recovery from a system failure or discontinuity of service. System crash can occur with inadequate mechanisms for secure recovery. User data objects and audit information may be modified or lost and system or application software may corrupted.

The TOE is unable to ensure recovery for IT other than itself. However, the TOE, as the underlying operating system, is expected to cooperate with its environment in accomplishing this recovery.

T.INSTALL: The system may be delivered or installed in a manner that undermines security.

The system security is predicated upon the IT being initially established in a secure state. That includes assurance that the TOE delivered is that which was evaluated and that the TOE, and other IT, is subsequently installed properly.

The TOE will be expected to provide significant support toward its own installation and toward the installation of other IT. However, due to the nature of the problem, significant support from the TOE's environment will be required in addressing this threat.

T.OPERATE: Security failures may occur because of improper operation; e.g., the abuse of authorized privileges.

The system security can be assured only to the extent that the TOE, and other IT, is operated correctly by system administrators and authenticated users in accordance with security policy. The

TOE will provide mechanisms that help mitigate this threat with respect to TOE operation and perhaps the operation of other IT. Additionally, specific environmental controls are still required for both the TOE and for other IT.

T.SYSTEM-CORRUPTED: The security state of the system, as a result of corruption of IT other than the TOE or as a result of a higher-grade attack, may be intentionally corrupted to enable future insecurities.

System security depends to a large degree on the integrity of the hardware and software implementing the security functionality. If this is intentionally corrupted, the IT will be unable to maintain a secure state. As an underlying operating system, the TOE will provide part of the protection for the system with respect to lower-grade threats. The TOE can only partially protect against higher-grade threats and may be able to only partially protect IT other than the TOE itself from lower-grade attacks. (See T.TOE-CORRPUTED for corruption of the TOE by lower-grade attacks.)

3.5 GENERAL ASSURANCE NEED

CSPP-OS compliant TOEs are targeted for near-term achievable, cost-effective, COTS security. In keeping with this target, the general level of assurance for CSPP-OS must:

- be consistent with current best commercial practice for IT development and
- enable evaluated products that are competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

CSPP-OS assurance must also, to enhance wide-spread acceptance, be consistent with current and near-term mutual recognition arrangement. This requires that the CSPP-OS assurances:

- be expressed as an existing evaluation assurance level (EAL) from part 3 of the Common Criteria; augmented by CC assurance components as required
- contain no assurance components first appearing in EAL5 or above

In keeping with these requirements, the general level of assurance needed for CSPP-OS is EAL2 augmented to include other vendor actions within the scope of current best commercial practice.

4. SECURITY OBJECTIVES

4.1 ENVIRONMENTAL SECURITY OBJECTIVES

Addressing some policies and threats is beyond the capabilities of the CSPP-OS compliant TOEs. This results in the environmental objectives listed in Table 4-1. The TOE does not contribute significantly to meeting these objectives.

The purpose of the environmental objectives (in conjunction with the Joint objectives) is to state what is expected of the TOE's environment in terms of risk mitigation or explicit risk acceptance.

Table 4-1 – Environmental Security Objectives

Environmental Security Objective	Corresponding Threat or Policy
O.ACCESS-NON-TECHNICAL: The TOE environment must provide sufficient protection against non-technical attacks by authenticated users for non-malicious purposes. This will be accomplished primarily via prevention with a goal of high effectiveness. Personnel security and user training and awareness will provide a major part of achieving this objective.	T.ACCESS-NON-TECHNICAL
O.ACCESS-Non-TOE: The IT other than the TOE must provide public access and access by authenticated users to the resources and actions for which they have been authorized and over which the TOE does not exercise control. The focus is on prevention with a high degree of effectiveness.	P.ACCESS
O.ACCOUNT-Non-TOE: The IT other than the TOE must ensure, for actions under its control or knowledge, that all users can subsequently be held accountable for their security relevant actions. This is expected with a high degree of effectiveness.	P.ACCOUNT T.TRACEABLE-Non-TOE T.RECORD-EVENT-Non-TOE T.AUDIT-CORRUPTED-Non-TOE T.AUDIT-CONFIDENTIALITY-Non-TOE
O.AUTHORIZE-Non-TOE: The IT other than the TOE must provide the ability to specify and manage user and system process access rights to individual processing resources and data elements under its control, supporting the organization's security policy for access control. This is expected with a high degree of effectiveness. NOTE: This includes initializing, specifying and managing (1) object security attributes, (2) active entity identity and security attributes, and (3) security relevant environmental conditions.	P.ACCESS

Environmental Security Objective	Corresponding Threat or Policy
O.AVAILABLE-Non-TOE: The IT other than the TOE must protect itself from unsophisticated, denial-of-service attacks. This is a combination of prevention and detect and recover with a high degree of effectiveness.	P.SURVIVE T.DENIAL-Non-TOE
O.BYPASS-Non-TOE: For access not controlled by the TOE, IT other than the TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing security policy enforcement. This will be accomplished with high effectiveness. NOTE: This objective is limited to 'non-malicious' because IT controls in the notional CSPP system are not expected to provide sufficient mitigation for the greater negative impact that 'malicious' implies.	T.ACCESS-Non-TOE
O.DENIAL-SOPHISTICATED: The TOE environment must maintain system availability in the face of sophisticated denial-of-service attacks. The focus is on detection and response with a goal of moderate effectiveness.	P.SURVIVE T.DENIAL-SOPHISTICATED
O.DETECT-SOPHISTICATED: The TOE environment must provide the ability to detect sophisticated attacks and the results of such attacks (e.g., corrupted system state). The goal is for moderate effectiveness.	P.SURVIVE T.SYSTEM-CORRUPTED
O.ENTRY-NON-TECHNICAL: The TOE environment must provide sufficient protection against non-technical attacks by other than authenticated users. This will be accomplished primarily via prevention with a goal of high effectiveness. User training and awareness will provide a major part of achieving this objective.	T.ENTRY-NON-TECHNICAL
O.ENTRY-Non-TOE: For resources not controlled by the TOE, IT other than the TOE must prevent logical entry using unsophisticated, technical methods, by persons without authority for such access. This is clearly a prevent focus and is to be achieved with a high degree of effectiveness.	P.USAGE T.ENTRY-Non-TOE
O.ENTRY-SOPHISTICATED: The TOE environment must sufficiently mitigate the threat of an individual (other than an authenticated user) gaining unauthorized access via sophisticated, technical attack. This will be accomplished by focusing on detection and response with a goal of moderate effectiveness.	T.ENTRY-SOPHISTICATED
O.INFO-FLOW: The TOE environment must ensure that any information flow control policies are enforced - (1) between system components and (2) at the system external interfaces. This will be accomplished by preventing unauthorized flows with high effectiveness.	P.INFO-FLOW
O.KNOWN-Non-TOE: The IT other than the TOE must ensure that, for all actions under its control and except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access. This is expected with a high degree of effectiveness.	P.KNOWN

Environmental Security Objective	Corresponding Threat or Policy
O.OBSERVE-Non-TOE: The IT other than the TOE must ensure that its security status is not misrepresented to the administrator or user. This is a combination of prevent and detect and, considering the potentially large number of possible failure modes, is to be achieved with a moderate, verses high, degree of effectiveness.	T.OBSERVE-Non-TOE
O.PHYSICAL: Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security. This will be accomplished primarily via prevention with a goal of high effectiveness.	P.PHYSICAL T.PHYSICAL

4.2 TOE SECURITY OBJECTIVES

While the environment contributes to the satisfaction of nearly all objectives, those listed here are satisfied by the TOE with only generic environmental support such as user training.

Table 4-2 gives the security objectives to be met by CSPP-OS compliant TOEs.

Table 4-2 – TOE Security Objectives

TOE Security Objective	Corresponding Threat or Policy
O.ACCESS-TOE: The TOE must provide public access and access by authenticated users to those TOE resources and actions for which they have been authorized. This will be accomplished with high effectiveness.	P.ACCESS
O.ACCOUNT-TOE: The TOE must ensure, for actions under its control or knowledge, that all TOE users can subsequently be held accountable for their security relevant actions. This will be done with moderate effectiveness, in that it is anticipated that individual accountability might not be achieved for some actions.	P.ACCOUNT T.TRACEABLE-TOE T.RECORD-EVENT-TOE T.AUDIT-CORRUPTED-TOE T.AUDIT-CONFIDENTIALITY-TOE
O.AUTHORIZE-TOE: The TOE must provide the ability to specify and manage user and system process access rights to individual processing resources and data elements under its control, supporting the organization's security policy for access control. This will be accomplished with high effectiveness. NOTE: This includes initializing, specifying and managing (1) object security attributes, (2) active entity identity and security attributes, and (3) security relevant environmental conditions.	P.ACCESS
O.AVAILABLE-TOE: The TOE must protect itself from unsophisticated, denial-of-service attacks. This will include a combination of protection and detection with high effectiveness.	P.SURVIVE T.DENIAL-TOE

TOE Security Objective	Corresponding Threat or Policy
O.BYPASS-TOE: The TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing TOE security policy enforcement. This will be accomplished with high effectiveness. NOTE: This objective is limited to 'non-malicious' because CSPP-OS controls are not expected to be sufficient mitigation for the greater negative impact that 'malicious' implies.	T.ACCESS-TOE
O.DETECT-TOE: The TOE must enable the detection of TOE specific insecurities. The goal is high effectiveness for lower grade attacks.	P.SURVIVE T.TOE-CORRUPTED
O.ENTRY-TOE: The TOE must prevent logical entry to the TOE using unsophisticated, technical methods, by persons without authority for such access. This will be accomplished with high effectiveness.	P.USAGE T.ENTRY-TOE
O.KNOWN-TOE: The TOE must ensure that, for all actions under its control and except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access. This will be accomplished with high effectiveness.	P.KNOWN
O.OBSERVE-TOE: The TOE must ensure that its security status is not misrepresented to the administrator or user. This is a combination of prevent and detect and, considering the potentially large number of possible failure modes, is to be achieved with a moderate, verses high, degree of effectiveness.	T.OBSERVE-TOE
O.RECOVER-TOE: The TOE must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity. This will be accomplished with a high effectiveness for specified failures and a low effectiveness for failures in general.	P.SURVIVE T.CRASH-TOE
O.RESOURCES: The TOE must protect itself from user or system errors that result in shared resource exhaustion. This will be accomplished via protection with high effectiveness.	P.SURVIVE T.RESOURCES

4.3 JOINT TOE/ENVIRONMENT SECURITY OBJECTIVES

The objectives listed here fall into one or more of the following categories:

a. The TOE and its environment together satisfy the objective as follows:

(1) TOE - contributes in a significant manner and

(2) Environment - contribution is specific to this objective; i.e, not the result of a general contribution such as user training.

b. At the level of abstraction of this PP either:

(1) It is not possible to accurately determine the split between TOE and environmental contribution, or

(2) Multiple, compliant solutions are feasible resulting in different mixes of TOE and environmental contributions

Table 4-3 – Joint TOE/Environment Security Objectives

Joint Security Objective	Corresponding Threat or Policy
O.ACCESS-MALICIOUS: The TOE controls will help in achieving this objective, but will not be sufficient. Additional, environmental controls are required to sufficiently mitigate the threat of malicious actions by authenticated users. This will be accomplished by focusing on deterrence, detection, and response with a goal of moderate effectiveness.	T.ACCESS-MALICIOUS
O.COMPLY: The TOE environment, in conjunction with controls implemented by the TOE, must support full compliance with applicable laws, regulations, and contractual agreements. This will be accomplished via some technical controls, yet with a focus on non-technical controls to achieve this objective with high effectiveness.	P.COMPLY
O.DETECT-SYSTEM: The TOE, in conjunction with other IT in the system, must enable the detection of system insecurities. The goal is high effectiveness for lower grade attacks.	P.SURVIVE T.SYSTEM-CORRUPTED
O.DUE-CARE: The TOE environment, in conjunction with the TOE itself, must be implemented and operated in a manner that clearly demonstrates due-care and diligence with respect to IT-related risks to the organization. This will be accomplished via a combination of technical and non-technical controls to achieve this objective with high effectiveness.	P.DUE-CARE
O.MANAGE: Those responsible for the system (in conjunction with mechanisms provided by the TOE) must ensure that it is managed and administered in a manner that maintains IT security. This will be accomplished with moderate effectiveness.	T.ADMIN-ERROR

O.NETWORK: The system must be able to meet its security objectives in a distributed environment. This will be accomplished with high effectiveness. Note: One mechanism that could help in addressing this objective is trusted path. However, COTS operating systems do not typically provide a trusted path between user and system and hence CSPP-OS does not require that the TOE provide it. Instead, when the TOE does not provide a trusted path, the protection that would have been provided by a trusted path is addressed by a combination of environmental controls such as add-on IT packages, non-technical controls (physical, procedural, personnel), and risk acceptance.	P.NETWORK
O.OPERATE: Those responsible for the system (in conjunction with mechanisms provided by the TOE) must ensure that the system is delivered, installed, and operated in a manner which maintains IT security. This will be accomplished with moderate effectiveness.	T.INSTALL T.OPERATE P.TRAINING
O.RECOVER-SYSTEM: The system must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity. This will be accomplished with some prevention and a majority of detect and respond, with high effectiveness for specified failures. For general failure, this will be accomplished with low effectiveness.	P.SURVIVE T.CRASH-SYSTEM

5. FUNCTIONAL SECURITY REQUIREMENTS

This section contains the functional requirements that must be satisfied by the notional CSPP system. These requirements consist of functional components from Part 2 of the CC, in some cases with modifications.

5.1 FUNCTIONAL REQUIREMENTS - TOE

Table 5-1 lists the functional requirements CSPP-OS compliant TOEs. All functional and assurance dependencies associated with the components in Table 5-1 have been satisfied.

Appendix B contains the explicit functional requirements that are summarized here.

Table 5-1 – Functional Components - TOE

Req Number	CC Component	Name	Extended	Refined	ST adds detail	Objectives function helps address
1	FAU_GEN.1-CSPP	Audit data Generation	x	x	x	O.ACCOUNT-TOE O.RECOVER-TOE O.RECOVER-SYSTEM O.DETECT-TOE O.DETECT-SYSTEM O.OPERATE O.MANAGE O.DUE-CARE
2	FAU_GEN.2	User Identity Generation		x		O.ACCOUNT-TOE
3	FAU_SAR.1	Audit Review				Required dependency for: FAU_SAR.2 FAU_SAR.3
4	FAU_SAR.2	Restricted Audit Review				O.BYPASS-TOE
5	FAU_SAR.3	Selectable Audit Review		x		O.ACCOUNT-TOE O.RECOVER-TOE O.RECOVER-SYSTEM O.DETECT-TOE O.DETECT-SYSTEM O.DUE-CARE O.OPERATE O.MANAGE O.COMPLY

Req Number	CC Component	Name	Extended	Refined	ST adds detail	Objectives function helps address
6	FAU_SEL.1-CSPP	Selective Audit	x	x		O.DUE-CARE O.DETECT-TOE O.DETECT-SYSTEM O.MANAGE O.OPERATE O.COMPLY
7	FAU_STG.1	Protected audit trail storage		x		O.DETECT-TOE O.DETECT-SYSTEM O.DUE-CARE O.COMPLY O.ACCOUNT-TOE O.BYPASS-TOE
8	FAU_STG.3	Action in case of Possible Audit Data Loss				O.ACCOUNT-TOE O.DUE-CARE O.MANAGE
9	FDP_ACC.1	Subset Access Control				O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.DUE-CARE O.COMPLY O.AVAILABLE-TOE O.RESOURCES
10	FDP_ACF.1-CSPP	Security Attribute Based Access Control	x	x		O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.DUE-CARE O.COMPLY O.AVAILABLE-TOE O.RESOURCES
11		CSPP requirement not applicable to this TOE				
12	FDP_ETC.1-CSPP	Export of user data without security attributes	x			O.BYPASS-TOE O.DUE-CARE O.ENTRY-TOE O.AVAILABLE-TOE
13		CSPP requirement not applicable to this TOE				
14		CSPP requirement not applicable to this TOE				
15	FDP_ITC.1	Import of user data without security attributes				O.NETWORK

Req Number	CC Component	Name	Extended	Refined	ST adds detail	Objectives function helps address
16		CSPP requirement not applicable to this TOE				
17	FDP_RIP.1	Subset Residual Information protection		x	x	O.BYPASS-TOE O.DUE-CARE
18		CSPP requirement not applicable to this TOE				
19	FDP_UCT.1	Basic data exchange confidentiality		x		O.NETWORK
20	FDP_UIT.1	Data exchange integrity		x		O.NETWORK
21	FIA_AFL.1	Authentication Failure Handling		x	x	O.DETECT-TOE O.DETECT-SYSTEM O.ENTRY-TOE O.BYPASS-TOE O.DUE-CARE O.COMPLY
22	FIA_ATD.1	User Attribute Definition		x	x	O.AUTHORIZE-TOE
23	FIA_SOS.1	Verification of Secrets		x	x	O.BYPASS-TOE O.DUE-CARE O.COMPLY
24		CSPP requirement not applicable to this TOE				
25	FIA_UAU.1	Timing of authentication		x	x	O.KNOWN-TOE
26	FIA_UAU.5	Multiple authentication mechanisms		x	x	O.NETWORK
27	FIA_UAU.6	Re-authenticating		x	x	O.BYPASS-TOE
28	FIA_UAU.7	Protected authentication feedback		x		O.BYPASS-TOE
29	FIA_UID.1	Timing of identification		x	x	O.KNOWN-TOE
30	FIA_USB.1	User-Subject Binding				O.ACCESS-TOE O.ACCESS-MALICIOUS O.DUE-CARE O.BYPASS-TOE
31	FMT_MOF.1	Management of security functions behavior		x	x	O.MANAGE O.DUE-CARE
32	FMT_MSA.1	Management of security attributes (includes iteration)		x	x	O.MANAGE O.DUE-CARE O.AUTHORIZE-TOE
33	FMT_MSA.3	Static attribute initialization				O.MANAGE O.DUE-CARE O.AUTHORIZE-TOE

Req Number	CC Component	Name	Extended	Refined	ST adds detail	Objectives function helps address
34	FMT_MTD.1	Management of TSF data		x		O.MANAGE O.DUE-CARE
35	FMT_SAE.1	Time-Limited Authorization		x	x	O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.AUTHORIZE-TOE O.MANAGE O.DUE-CARE
36	FMT_SMR.1	Security roles		x	x	O.MANAGE O.DUE-CARE
37	FPT_AMT.1	Abstract Machine Testing		x		Required dependency for: FPT_TST.1
38	FPT_FLS.1	Failure with preservation of secure state		x	x	O.RECOVER-TOE O.RECOVER-SYSTEM
39	FPT_ITC.1-CSPP	Inter-TSF Confidentiality During Transmission	x	x		O.NETWORK
40	FPT_ITI.1-CSPP	Inter-TSF detection of modification (operations – TBD)	x	x	x	O.NETWORK
41		CSPP requirement not applicable to this TOE				
42	FPT_RCV.2	Automated Recovery		x	x	O.RECOVER-TOE O.RECOVER-SYSTEM
43	FPT_RPL.1-CSPP	Replay detection (operations – TBD)	x	x	x	O.NETWORK
44	FPT_RVM.1	Non-Bypassability of the TSP		x		O.BYPASS-TOE
45	FPT_SEP.1	TSF Domain Separation		x		O.BYPASS-TOE O.DUE-CARE
46	FPT_TDC.1	Inter-TSF basic TSF data consistency (operations – TBD)		x	x	O.NETWORK
47		CSPP requirement not applicable to this TOE				
48	FPT_TST.1	TSF Testing		x		O.DETECT-TOE O.DETECT-SYSTEM O.DUE-CARE
49	FRU_RSA.1-CSPP	Maximum quotas (operations – TBD)		x	x	O.RESOURCES

Req Number	CC Component	Name	Extended	Refined	ST adds detail	Objectives function helps address
50	FTA_LSA.1	Limitation on scope of selectable attributes (operations – TBD)		x	x	O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.DUE-CARE
51	FTA_MCS.1-CSPP	Basic limitation on multiple concurrent session	x	x		O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.DUE-CARE
52	FTA_SSL.1	TSF-initiated session locking				O.BYPASS-TOE O.DUE-CARE
53	FTA_SSL.2	User-initiated locking				O.OPERATE O.BYPASS-TOE O.DUE-CARE
54	FTA_SSL.3	TSF-initiated termination				O.BYPASS-TOE O.DUE-CARE
55	FTA_TAB.1-CSPP	Default TOE access banners	x			O.ENTRY-TOE O.ACCOUNT-TOE O.DUE-CARE O.COMPLY
56	FTA_TAH.1	TOE access history		x		O.OBSERVE-TOE O.ENTRY-TOE O.BYPASS-TOE O.DUE-CARE O.COMPLY
57	FTA_TSE.1	TOE session establishment (operations – TBD)		x	x	O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE
58	FTP_ITC.1-CSPP	Inter-TSF trusted channel (operations – TBD)	x	x	x	O.NETWORK
59		CSPP requirement not applicable to this TOE				
60	Non-CC FPT_SYN-CSPP.1	TSF synchronization Component defined in [CSPP] FPT_STM.1 changed to be synchronization requirements (instead of just requiring a mechanism that supports it)	x	x		O.NETWORK

5.2 FUNCTIONAL REQUIREMENTS - IT ENVIRONMENT

This section describes what is known about the functional requirements that the IT in the environment surrounding the TOE must provide in order for the environmental and joint security objectives to be met. For an operating system this equates to requirements placed upon the underlying hardware/firmware platform.

Table 5-2 – Functional Components - IT Environment

Req Number	CC Component	Name	Objectives function helps address
7	FAU_STG.1	Protected audit trail storage	O.DETECT-SYSTEM O.DUE-CARE O.COMPLY O.ACCOUNT-NON-TOE O.BYPASS-NON-TOE
9	FDP_ACC.1	Subset Access Control	O.ACCESS-NON-TOE O.ENTRY-NON-TOE O.DUE-CARE O.COMPLY O.AVAILABLE-NON-TOE
17	FDP_RIP.1	Subset Residual Information protection	O.BYPASS-NON-TOE O.DUE-CARE
25	FIA_UAU.1	Timing of authentication	O.KNOWN-NON-TOE
27	FIA_UAU.6	Re-authenticating	O.BYPASS-NON-TOE
28	FIA_UAU.7	Protected authentication feedback	O.BYPASS-NON-TOE
31	FMT_MOF.1	Management of security functions behavior	O.MANAGE O.DUE-CARE
33	FMT_MSA.3	Static attribute initialization	O.MANAGE O.DUE-CARE O.AUTHORIZE-NON-TOE
34	FMT_MTD.1	Management of TSF data	O.MANAGE O.DUE-CARE
37	FPT_AMT.1	Abstract Machine Testing	Required dependency for: FPT_TST.1
42	FPT_RCV.2	Automated Recovery	O.RECOVER-SYSTEM
44	FPT_RVM.1	Non-Bypassability of the TSP	O.BYPASS-NON-TOE
45	FPT_SEP.1	TSF Domain Separation	O.BYPASS-NON-TOE O.DUE-CARE

Req Number	CC Component	Name	Objectives function helps address
56	FTA_TAH.1	TOE access history	O.OBSERVE-NON-TOE O.ENTRY-NON-TOE O.BYPASS-NON-TOE O.DUE-CARE O.COMPLY
60	Non-CC FPT_SYN-CSPP.1	TSF synchronization FPT_STM.1 changed to be synchronization requirements (instead of just requiring a mechanism that supports it)	O.NETWORK

5.3 NON-IT ENVIRONMENTAL FUNCTIONAL REQUIREMENTS

The environment is required to satisfy the secure usage assumptions in Section 3.2, meet all of the environmental security objectives outlined in section 4.1, and support the objectives in section 4.3. The specific, non-IT functional requirements are not identified in this PP. The higher-level objective statements are considered sufficient for determining the adequacy of non-IT environmental support.

The following objectives are covered, almost exclusively, by non-IT environmental controls:

O.ACCESS-NON-TECHNICAL

O.DENIAL-SOPHISTICATED

O.DETECT-SOPHISTICATED

O.ENTRY-NON-TECHNICAL

O.ENTRY-SOPHISTICATED

O.PHYSICAL

The following objectives receive significant coverage by non-IT environmental controls:

O.ACCESS-MALICIOUS

O.COMPLY

O.DUE-CARE

O.MANAGE

O.OPERATE

5.4 STRENGTH OF FUNCTION (SOF)

This section is required by the Common Criteria and specifies the strength of function necessary to accomplish the intent of this PP. Both a minimum level for the PP as a whole and specific metrics for individual functions are provided.

Note that, while not probabilistic, SOF metrics have been given for FAU_STG.1, FDP_RIP.1, FMT_MTD.1, and FPT_SEP.1. This extension of the CC with respect to SOF, is being used as a convenient means of capturing all "strength" elements in a common location of the PP.

5.4.1 Minimum SOF Requirement

As the goal for CSPP-OS is near-term achievable COTS, the appropriate minimum SOF level is **BASIC**.

5.4.2 Specific SOF Requirements - TOE

The specific required strength metrics for the functional components are given in Table 5-3.

Table 5-3 – SOF Metrics - TOE

#	CC Component	Name	Explicit SOF Metric
19	FDP_UCT.1	Basic data exchange confidentiality	support equivalent or stronger: 1024 bit key exchange and triple DES or better (as well as weaker values as required by import/export restrictions)
20	FDP_UIT.1	Data exchange integrity	MD5 or stronger checksums will be used
23	FIA_SOS.1	Verification of Secrets	FIPS PUB 112
39	FPT_ITC.1-CSPP	Inter-TSF Confidentiality During Transmission	support equivalent, or stronger: 1024 bit key exchange and triple DES (as well as weaker values as required by import/export restrictions)
40	FPT_ITI.1-CSPP	Inter-TSF detection of modification	MD5 equivalent or stronger checksums will be used
45	FPT_SEP.1	TSF Domain Separation	use underlying hardware ring structure to separate, at a minimum, kernel space from application space
48	FPT_TST.1	TSF Testing	MD5 or stronger checksums will be used

5.4.3 Specific SOF Metrics - IT Environment

Table 5-4 gives the SOF metrics for functional requirements placed on the IT-environment.

Table 5-4 – SOF Metrics - IT Environment

#	CC Component	Name	Explicit SOF Metric
7	FAU_STG.1	Protected audit trail storage	provide a hardware protected copy of the audit trail, allowing 'append' as the only write access
17	FDP_RIP.1	Subset Residual Information protection	applications will take advantage of OS supplied mechanisms
34	FMT_MTD.1	Management of TSF data	include operating system access controls in controlling access to TSF critical data
45	FPT_SEP.1	TSF Domain Separation	use underlying hardware ring structure to separate, at a minimum, kernel space from application space

6. ASSURANCE REQUIREMENTS

The assurance requirements for CSPP-OS are met by an augmented EAL2 that is henceforth termed evaluation assurance level – CSPP (EAL-CSPP). EAL-CSPP stresses assurance through vendor actions that are within the bounds of current best-commercial-practice. EAL-CSPP provides, primarily via review of vendor supplied evidence, independent confirmation that these actions have been competently performed. EAL-CSPP also includes the following independent, third-party analysis: (1) confirmation of system generation and installation procedures, (2) verification that the system security state is not misrepresented, (3) verification of a sample of the vendor functional testing, (4) searching for obvious vulnerabilities, and (5) independent functional testing.

The assurance components for EAL-CSPP are summarized in Table 6-1. Appendix C gives the details of these assurance components. Table 6-2 lists those components of EAL-CSPP that augment EAL2 from part 3 of the CC.

Table 6-1 – EAL-CSPP Assurance Components

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.3	Authorization controls
	ACM_SCP.2	Problem tracking CM Coverage
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, Generation, and Start-up Procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive High-Level Design
	ADV_RCR.1	Informal Correspondence Demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator Guidance
	AGD_USR.1	User Guidance
Life Cycle Support	ALC_DVS.1	Identification of Security Measures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing - High-Level Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_MSU.2	Validation of Analysis
	AVA_SOF.1	Strength of TOE Security Function Evaluation
	AVA_VLA.1	Developer vulnerability Analysis

Table 6-2 – EAL-CSPP augmentation to EAL-2

EAL2	EAL-CSPP	Nature of Augmentation to EAL2
ACM_CAP.2	ACM_CAP.3	• requires a CM plan • describe how plan is used • provide evidence that – CM is operating in accordance with plan – configuration items are being effectively maintained – only authorized changes are made to configuration items
none	ACM_SCP.2	• CM documentation shows that CM system tracks – TOE implementation – design documentation – test documentation – user and administrator documentation – CM documentation – security flaws • CM documentation describes how configuration items are tracked
none	ADV_SPM.1	• provide an informal TOE security policy model that – describes rules and characteristics of all policies that can be modeled. – includes a rationale demonstrating consistency and completeness with respect to these policies • show consistency and completeness between all security functions in the functional specification and the model
none	ALC_DVS.1	• produce developmental security documentation that – describes the security measures necessary {in the opinion of the developer} to provide, for the TOE design and implementation, what confidentiality and integrity the developer considers necessary – provides evidence that these measures are being followed during TOE development and maintenance • evaluator confirms that the security measures identified are being applied Note: The evaluator does not, at ALC_DVS.1, confirm that the list of security measures in adequate. That is added at the next higher component (ALC_DVS.2).

EAL2	EAL-CSPP	Nature of Augmentation to EAL2
none	ALC_FLR.2	• establish procedure for accepting and action upon user reports of security flaws • document flaw remediation procedures – describing procedures used to track security flaws – describing methods to provide flaw information, corrections, and guidance to users – requiring that description of and effect of flaw be provided – requiring that corrective actions be identified and correction status be provided – ensuring that reported flaws are corrected and corrections issued to users – providing safeguards that any corrections do not introduce new flaws
ATE_COV.1	ATE_COV.2	• requirement for developer analysis of test coverage – changing, for correspondence between test coverage and the functional specification, “evidence … show” to “analysis … demonstrate” • requirement that the coverage is ‘complete’
none	ATE_DPT.1	• requirement for developer analysis of test depth – depth sufficient to demonstrate operates in accordance with high-level design
none	AVA_MSU.2	• requirements placed upon guidance documentation – identify all possible modes of operation, their consequences and implications toward secure operation – be complete, clear, consistent, and reasonable – list all assumptions about the intended environment – list all requirements for external security measures • developer analysis of guidance documentation for completeness • evaluator confirmation of analysis of documentation completeness

7. APPLICATION NOTES

7.1 EVALUATION SCOPE, DEPTH, AND RIGOR.

In lieu of extensive, independent analysis, CSPP-OS intends the evaluator to:

a. Review developer supplied evidence to make a determination on:
   i) the competence of the vendor
   ii) the apparent correctness and completeness of the required security actions

b. Approach all requirements to ensure “all”, “any”, or “none” as generic CC requirements to be interpreted loosely when applied to this lower assurance evaluation.

c. Be consciously aware that there is a point at which more evaluation is not cost-effective; keeping in mind that CSPP-OS is a lower assurance, lower cost, basic level of security.

This intention to limit independent analysis directly applies to the following assurance elements:

a. ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

b. ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

c. ADV_IND.2.2E The evaluator shall test the TSF to confirm that the TSF operates as specified.

d. AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

e. AVA_MSU.2.4E The evaluator shall confirm that the analysis shows that guidance is provided for secure operation in all modes of operation of the TOE.

f. AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

g. AMA_CAT.1.2E The evaluator shall confirm that the categorization of TOE components and tools, and the categorization scheme used, are appropriate and consistent with the evaluation results for the certified version.

8. RATIONALE

The rationale for this PP guidance is found in [CSPP-OS-R].

9. REFERENCES

[CC-V2.1] *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999.

[CSPP] *CSPP - Guidance for COTS Security Protection Profiles*, version 1.0, December 1999.

[CSPP-OS-R] *Rationale for CSPP-OS - COTS Security Protection Profile* - Operating Systems, version 0.3, April 2000.

A. APPENDIX A: ACRONYMS

CC	Common Criteria [for IT Security Evaluation]
COTS	Commercial Off The Shelf
EAL	Evaluation Assurance Level
IT	Information Technology
NIST	National Institute of Standards and Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

B. APPENDIX B: TOE FUNCTIONAL REQUIREMENT DETAILS

B.1 COMMON SYNTAX

Throughout this section the following terminology is used:

Completed operations:
Selection: [**selection:** selection made]
Assignment: [**assignment:** assignment made]
Refinement: <u>refinement made</u>
Extension: either [**extension:** extension made] or title indicating following is an extension

Deferred operations are shown in italics, for example:
Deferred assignment: *[**ST assignment:** description of operation to be performed]*

B.2 CSPP ACCESS CONTROL SECURITY FUNCTION POLICY (SFP)

The TOE shall support the administration and enforcement of the an access control SFP that provides at least the equivalent of the following two capabilities described below, in accordance with the precedence rules indicated.

B.2.1 Discretionary Access Control

Subjects (human users operating through software processes and software processes running as system processes) will be granted access to objects (files) based upon authorizations associated with the object being accessed, the name of the subject requesting access, the type of access requested, and the nature of the access request.

Authorizations associated with each object define allowed accesses by:

Subject identification:
Multiple individuals with potentially different access authorizations
Multiple subject groups with potentially different access authorizations

Access type, with explicit allow or deny:
Read
Write
Execute

Nature of access:
Time of day
Port of entry

For each object, an explicit owning subject (or group of subjects) will be identified.

For each object, the assignment and management of authorizations will be the responsibility of the owner of that object and, if the implementation allows, other subjects may be explicitly granted the privilege of modifying the object's authorizations.

The system is allowed to provide a privileged user or user role that can bypass all access controls; for example the Unix 'root' or NT 'administrator'.

B.2.2 Non-discretionary Access Controls

a. The ability of a software process to access key system resources; for example external ports, input output capabilities, and operating system data structures; will be restricted based upon the assigned processing level of the process within a multiple ring architecture of the underlying hardware platform. A compliant security target will include a definition of key resources and a justification for the operating system architecture, displaying how allocation of OS processes and user processes between ring levels enforces non-discretionary access controls to key resources.

b. System level access controls set by explicitly authorized users such as a security adminstrator, and not modifiable by the asset owner. These include controls related to:

Nature of access, for example:
Time of day
Port of entry

Authentication mechanism(s) required

B.2.3 CSPP Access Control Precedence Rules

CSPP-OS compliant TOEs will determine allowed access for a specific subject to a specific object according to these precedence of rules:

1) If the requested mode of access is denied to that subject, deny access.

2) If the requested mode of access is permitted to that subject, permit access.

3) If the requested mode of access is denied to every group of which the user is a member, deny access

4) If the requested mode of access is permitted to any group of which the user is a member, grant access

5) If the requested mode of access is denied to public, deny access

6) If the requested mode of access is permitted to public, grant access

7) Else deny access.

B.3 AUDIT (FAU)

B.3.1 FAU_GEN.1-CSPP Audit data generation

Dependencies: FPT_STM.1 (FPT_SYN-CSPP.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events relevant for the [**selection:** basic] level of audit; and

c) [**assignment:**

(1) for FPT_ITI.1 and FPT_RPL.1, the ability to provide statistical data representing the frequency of occurrence and

(2) other auditable events specific to the ST design as listed in the following ST assignment: ***[ST assignment:*** *any other audit events required by specifics of the ST design in order to meet PP requirements.]*] The ST rationale shall provide a basic justification, showing that the ST assignment, to include a “null” assignment, is complete.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (human user/software process), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**assignment:** “none”].

Extension:

FAU_GEN.1-CSPP.3 When the TSF provides application support it shall support an application program interface (API) that allows a privileged application to append data to the security audit trail or to an application-specified alternative security audit trail.

Refinement: See text in FAU_GEN.1.1 and FAU_GEN.1.2

B.3.2 FAU_GEN.2 User identity generation

Dependencies: FAU_GEN.1-CSPP, FIA_UID.1

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the individual identity of the user or system process that caused the event.

Refinement: See text of FAU_GEN.2.1

B.3.3 FAU_SAR.1 Audit review

Dependencies: FAU_GEN.1-CSPP

FAU_SAR.1.1 The TSF shall provide [**assignment:** explicitly authorized user roles, user groups, or individually identified users] with the capability to read [**assignment:** all information in the audit records] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

B.3.4 FAU_SAR.2 Restricted audit review

Dependencies: FAU_SAR.1

FAU_SAR_2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

B.3.5 FAU_SAR.3 Selectable audit review

Dependencies: FAU_SAR.1

FAU_SAR.3.1 The TSF shall provide the ability to perform [**selection:** searches, sorting, and ordering] of audit data based upon [**assignment:** at a minimum, date and time of the event, subject (user or process), type of event, and success or failure].

Refinement: See text of FAU_SAR.3.1

B.3.6 FAU_SEL.1-CSPP Selective audit

Dependencies: FAU_GEN.1-CSPP
FMT_MTD.1

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
a) [**selection:** Object identity, user identity, subject identity, host identity, and/or event type];
b) [**assignment:** success or failure.]

Extension:

FAU_SEL.1-CSPP.2 The TSF shall provide only explicitly authorized user roles, user groups, or individually identified users with the ability to select or display which events are to be audited.

FAU_SEL.1-CSPP.3 The TSF shall provide the capability of FAU_SEL.1-CSPP.2 at any time during the operation of the TOE.

Refinement: See text of FAU_SEL1.1

B.3.7 FAU_STG.1 Protected audit trail storage

Dependencies: FAU_GEN.1-CSPP

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [**selection:** prevent and detect] modifications to the audit records.

Refinement: See text in FAU_STG.1.2

B.3.8 FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1

FAU_STG.3.1 The TSF shall take [**assignment:** the action to notify an identified user or console of the possible audit data loss] if the audit trail exceeds [**assignment:** an authorized user selectable, pre-defined limit].

B.4 USER DATA PROTECTION (FDP)

B.4.1 FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1-CSPP

FDP_ACC.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP] on [**assignment:** all subjects, all operating system controlled files (to include all communications mechanisms – for internal or external communications – that are implemented as objects controlled by the file system), and all access requests to these files].

B.4.2 FDP_ACF.1-CSPP Security attribute based access control

Dependencies: FDP_ACC.1, FMT_MSA.3

FDP_ACF.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP] to objects based on [**assignment:** user/process identity, group membership, subject privileges, and, if included in the object authorization information, access restrictions such as the time-of-day and port-of-entry].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed [**assignment:** by checking the authorizations associated with the object for the entries of that subject].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**assignment:** none].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the <u>following additional rules:</u> [**assignment:** none].

Extension:

FDP_ACF.1-CSPP.5 The TSF shall provide the capability to assign a user to be a member of more than one user group simultaneously.

FDP_ACF.1-CSPP.6 The TSF shall enforce the rules for authorizing and denying access based upon the CSPP precedence rules.

Refinement: See text in FDP_ACF.1.4

B.4.3 FDP_ETC.1-CSPP Export of user data without security attributes

Dependencies: FDP_ACC.1 or- FDP_IFC.1

FDP_ETC.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP] when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

Extension:

FDP_ETC.1-CSPP.3 The TSF shall shall provide for outgoing information channels, for example TCP port numbers, that are under the control of the TSF and for which general application programs do not have access, when exporting user data controlled under the SFP outside the TSC.

B.4.4 FDP_ITC.1 Import of user data without security attributes

Dependencies: FDP_ACC.1 or/and FDP_IFC.1, FMT_MSA.3

FDP_ITC.1.1 The TSF shall enforce the [**assignment:** CSPP access control] when importing user data, controlled under the SFP, from outside the TSC.

FDP_ITC.1.2 The TSF shall ignore the security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following the following rules when importing user data controlled under the SFP from outside the TSC: [**assignment:** the TOE shall provide for incoming information channels, for example TCP port numbers, that are under the control of the TSF and for which general application programs do not have access].

B.4.5 FDP_RIP.1 Subset residual information protection

Dependencies: None

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**assignment:** following: *[**ST selection:** allocation of the resource to, deallocation of the resource from, both]*] the following objects [**assignment:** shared memory and file storage space]. The ST rationale shall provide a basic justification, showing that the ST selection is consistent with other aspects of the ST design, resulting in a secure solution.

Refinement: See text in FDP_RIP.1.1

B.4.6 FDP_UCT.1 Basic data exchange confidentiality

Dependencies: FTP_ITC.1-CSPP or FTP_TRP.1-CSPP, FDP_ACC.1

FDP_UCT.1.1 The TSF shall support the enforcement of the [**assignment:** CSPP access control SFP] to be able to [**selection:** transmit and receive] objects in a manner protected from unauthorized disclosure.

Refinement: See text in FDP_UCT.1.1

B.4.7 FDP_UIT.1 Data exchange integrity

Dependencies: FTP_ITC.1-CSPP or FTP_TRP.1-CSPP, FDP_ACC.1

FDP_UIT.1.1 The TSF shall support the enforcement of the [**assignment:** CSPP access control SFP] to be able to [**selection:** transmit and receive] user data in a manner protected from [**selection:** modification, deletion, insertion, and replay] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [**selection:** modification, deletion, insertion, or replay] has occurred.

Refinement: See text in FDP_UIT.1.1 and FDP_UIT.1.2

B.5 IDENTIFICATION AND AUTHENTICATION (FIA)

B.5.1 FIA_AFL.1 Authentication failure handling

Dependencies: FIA_UAU.1

FIA_AFL.1.1 The TSF shall detect when [**assignment:** an authorized user configurable number of] unsuccessful authentication attempts over an authorized user configurable length of time occur related to [**assignment:** initial account login, re-authentication after initial login, and list of other events given in the following ST assignment: *[**ST assignment:** as required by PP, list of ST specific authentication events]*]. The ST rationale shall provide a basic justification that the ST assignment, including a "null" assignment, includes all events specific to the ST design that require authentication failure handling.

FIA_AFL.1.2 After the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**assignment:** perform the following ST selected actions: *[**ST selection:** disable the account (requiring it to be re-enabled by an authorized user), cause each subsequent logon attempt to be delayed for increasing periods of time up to a maximum number of additional attempts at which time the account is disabled pending authorized user action to re-enable, allow either option based upon a configuration choice by an authorized user]*]. As any selection, other than "null", is acceptable and the purpose here is to ensure that an explicit choice is both made and announced, the ST rationale need not justify the choice made.

Refinement: See text of FIA_AFL.1.1 and FIA_AFL.1.2

B.5.2 FIA_ATD.1 User attribute definition

Dependencies: None

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**assignment:** user name, authenticator and the following ST specific attributes required by the design of the ST: *[**ST assignment:** as required by PP, list of any ST specific security attributes]*]. The ST rationale shall provide a basic justification for the assignment made, including "null", showing that it is the complete list required to maintain secure operation.

Refinement: See text in FIA_ATD.1.1

B.5.3 FIA_SOS.1 Verification of secrets

Dependencies: None

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**assignment**: for passwords, the application note below and the requirements of FIPS PUB 112; for other secrets specific to the ST design, the metrics called out in the following ST assignment: *[**ST assignment:** as required by PP, any ST specific, defined quality metrics]*]. The ST rationale shall provide a basic justification that the ST assignment covers all ST specific secrets essential for secure operation and that the metric(s) given are appropriate for meeting the PP design goals.

Refinement: See text in FIA_SOS.1.1

Application note. Elements for security quality metric related to passwords include:

a. Passwords shall not be reusable by the same user identifier for a period of time that can be set by an authorized user.

b. The TSF shall not indicate to the user if he/she has chosen a password already associated with another user.

c. The TSF shall, by default, prohibit the use of null passwords during normal operation.

d. The TSF shall provide an algorithm for ensuring the complexity of user-entered passwords that meets the following requirements:

   i. Passwords shall meet an authorized user specifiable minimum length requirement. The default minimum length shall be eight characters.

   ii. The password complexity-checking algorithm shall be modifiable by the TSF. The default algorithm shall require passwords to include at least one alphabetic character, one numeric character, and one special character.

   iii. The TSF should provide a protected mechanism that allows systems to specify a list of excluded passwords (e.g., company acronyms, common surnames).

   iv. The TSF should prevent users from selecting a password that matches any of those on the list of excluded passwords.

B.5.4 FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1

FIA_UAU.1.1 The TSF shall allow [**assignment:** no actions other than anonymous access to resources explicitly authorized for the type of anonymous access requested and the following ST selection *[**ST selection:** as permitted by PP, local shut down of the operating system]*] on behalf of the user to be performed before the user is authenticated. As the inclusion of this action is permitted, but not required, and the purpose here is only to ensure that the ST choice is explicit, the ST rationale does not need to include a justification for the choice made.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of the user.

Refinement: See text in FIA_UAU.1.1

B.5.5 FIA_UAU.5 Multiple authentication mechanisms

Dependencies: None

FIA_UAU.5.1 The TSF shall provide support for [**assignment:** the required use of authentication mechanisms other than only passwords, based upon access parameters such as time of day, port of entry, and user privilege] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**assignment:** parameters for selecting authenticators required, these parameters are to be specifiable by an explicitly specified set of users, enforcing least privilege on the basis of the following ST selection: *[**ST selection:** explicitly authorized security administrators, security administrator roles, both]*]. The ST rationale shall provide a basic justification for the selection made, indicating how it supports enforcement of least privilege.

Refinement: See text in FIA_UAU.5.1 and FIA_UAU.5.2

B.5.6 FIA_UAU.6 Re -authentication

Dependencies: None

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [**assignment:** re-establishing a session following session locking, request to change authentication secrets, and the following ST supplied conditions specific to the ST design: *[**ST assignment:** as required by PP, list of other, ST specific conditions under which re-authentication is required]*]. The ST rationale shall provide a basic justification for the assignment made, including a "null" list, showing why it is complete.

Refinement: See text in FIA_UAU.6.1

B.5.7 FIA_UAU.7 Protected authentication feedback

Dependencies: FIA_UAU.1

FIA_UAU.7.1 The TSF shall not provide [**assignment:** any indication of success or failure nor clear-text display of any secret authenticator] to the user while the authentication is in progress.

Refinement: See text in FIA_UAU.7.1

B.5.8 FIA_UID.1 Timing of identification

Dependencies: None

FIA_UID.1.1 The TSF shall allow [**assignment:** no actions other than anonymous access to resources explicitly authorized for the type of anonymous access requested and the following ST selection *[**ST selection:** as allowed by PP, local shut down of the operating system]*] on behalf of the user to be performed before the user is identified. As the operation is permitted rather than required, and the purpose here is to ensure that the choice is explicit, the ST rationale does not need to include a justification for the choice made.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Refinement: See text in FIA_UID.1.1

B.5.9 FIA_USB.1 User-subject binding

Dependencies: FIA_ATD.1

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

B.6 SECURITY MANAGEMENT (FMT)

B.6.1 FMT_MOF.1 Management of security functions behavior

Dependencies: FMT_SMR.1

FMT_MOF.1.1 The TSF shall restrict the ability to [**selection:** determine the behaviour of, disable, enable, modify the behavior of] the functions [**assignment:** included as requirements for CSPP-OS and for which the common criteria indicates security management suggestions, and also all items listed in the following ST assignment: *[**ST assignment:** as required by PP, list of ST functions and mechanisms resulting from specifics of the ST design]*] to [**assignment:** an explicitly specified set of users, enforcing least privilege on the basis of the following ST selection: *[**ST selection:** security administrators, security administrator roles, both]*]. The ST rationale must provide a basic justification for the assignment made, to include "null". The ST rationale must also provide a basic justification for the selection made, indicating how it supports enforcement of least privilege.

Refinement: See text in FMT_MOF.1.1

B.6.2 FMT_MSA.1 Management of security attributes

Dependencies: FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1

FMT_MSA.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP] to restrict the ability to [**selection:** change_default, modify, delete] and [**assignment:** "null"] the security attributes [**assignment:** all attributes used to define the security state of the system, to control the security functionality, to make access control decisions, and those listed in the following ST assignment: *[**ST assignment:** as required by PP, list of security attributes requiring management and arising from the specifics of the ST design]*] to [**assignment:** for discretionary attributes, the owner of the attribute; for both discretionary and non-discretionary attributes, an explicitly specified set of users, enforcing least privilege on the basis of the following ST selection: and *[**ST selection:** security administrators, security administrator roles, both]*]. The ST rationale shall provide a basic rationale for the assignment made, showing it to be complete. Also, the ST rationale shall provide a basic justification for the selection made, indicating how it enforces least privilege. See iteration for restriction on read access to authenticator values.

Iteration:

FMT_MSA.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP] to restrict the ability to [**selection:** query] [**assignment:** "null"] the security attributes [**assignment:** current and past values of authenticators,] to [**assignment:** no users and only to software processes requiring this knowledge].

Application note: An example of a processes requiring this information is a password change function which will query for current password and must make a determination as to whether the password entered is correct.

Refinement: See text in first iteration of FMT_MSA.1.1

B.6.3 FMT_MSA.3 Static attribute initialization

Dependencies: -FMT_MSA.1, FMT_SMR.1

FMT_MSA.3.1 The TSF shall enforce the [**assignment:** CSPP access control SFP] to provide [**assignment:** restrictive] default values for object security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**assignment:** data object owner and other authorized users] to specify alternate initial values to override the default values when an object or information is created.

B.6.4 FMT_MTD.1 Management of TSF data

Dependencies: FMT_SMR.1

FMT_MTD.1.1 The TSF shall restrict the ability to [**selection:** change_default, read, modify, delete, or clear] the [**assignment:** all internal TSF data structures that are security critical] to [**assignment:** software processes explicitly authorized to access this data].

Refinement: See text in FMT_MTD.1.1

B.6.5 FMT_SAE.1 Time-limited authorization

Dependencies: FMT_SMR.1, FMT_STM.1 (FMT_CSPP-OS.1)

FMT_SAE.1.1 The TSF shall restrict the ability to specify an expiration time for [**assignment:** user account and authenticators and *[**ST assignment:** as required by PP, list of ST specific security attributes for which expiration is to be supported]*] to [**assignment:** an explicitly specified set of users, enforcing least privilege on the basis of the following ST selection: *[**ST selection:** security administrators, security administrator roles, both]*]. The ST rationale shall provide a basic justification for the assignment made, to include a "null" assignment, showing that it is a complete list with respect to the attributes which must be restricted to enforce secure operation. The ST rationale shall also provide a basic justification for the selection made, indicating how it enforces least privilege.

FMT_SAE.1.2 For each of these security attributes, TSF shall be able to [**assignment:** for user account - disable account and require administrator action to re-enable, for authenticators - require owner of authenticator to establish a new value before proceeding with authenticated action] and *[**ST assignment:** as required by PP, list of ST specific actions to be taken for each ST specific security attribute]* after the expiration time for the indicated security attribute has passed. The ST rationale shall provide a basic justification for the assignment made, to include "null", showing that it is sufficient to enable secure operation.

Refinement: See text in FMT_SAE.1.1 and FMT_SAE.1.2

B.6.6 FMT_SMR.1 Security roles

Dependencies: FIA_UID.1

FMT_SMR.1.1 The TSF shall maintain the roles [**assignment:** privileged user (for example the equivalent of the Unix root) and/or the following set of ST specific roles that the ST author wishes to specify as not conflicting with CSPP goals and useful in implementing these goals: *[**ST assignment:** as allowed by PP, the ST specific authorized identified roles]*]. The ST rationale shall provide a basic justification for the assignment made, showing that the roles specified do not conflict with PP design goals.

FMT_SMR.1.2 The TSF shall be able to associate users the roles.

Refinement: See text in FMT_SMR.1.1

B.7 PROTECTION OF TRUSTED SECURITY (FPT)

B.7.1 FPT_AMT.1 Abstract machine testing

Dependencies: None

FPT_AMT.1.1 The TSF shall run a suite of tests [**selection:** during initial start-up and at the request of explicitly authorized security administrator(s) or security administrator role(s)] to demonstrate the correct operation of the security assumptions provided by the abstract machine which underlies the TSF.

Refinement: See text in FPT_AMT.1.1

B.7.2 FPT_FLS.1 Failure with preservation of secure state

Dependencies: ADV_SPM.1

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [**assignment:** those indicated in the following ST assignment: *[**ST assignment:** list of TSF failures for which the ST is able to preserve a secure state]*]. As the purpose of this requirement is to make the list of recoverable failures explicit, not to mandate specific failures, the ST rationale does not need to show completeness. However, the ST rationale does need to provide a basic justification for the claim that the ST will preserve a secure state for each failure type listed.

Refinement: See text in FPT_FLS.1.1

B.7.3 FPT_ITC.1-CSPP Inter-TSF confidentiality during transmission

Dependencies: None

FPT_ITC.1.1-CSPP The TSF shall support the protection of [**extension:** authentication information] transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

Refinement: See text of FPT_ITC.1.1-CSPP
Extension: See text of FPT_ITC.1.1-CSPP

B.7.4 FPT_ITI.1-CSPP Inter-TSF detection of modification

Dependencies: None

FPT_ITI.1.1-CSPP The TSF shall support the capability to detect modification of [**extension:** security state information that is critical to maintaining a secure state among distributed systems as identified in *[**ST assignment:** list of TSF data requiring such protection]*] data during transmission between TSF and a remote trusted IT product within the following metric: *[**ST assignment**: a defined modification metric or metrics]*. [**extension:** The first ST assignment may be a ‘null’ list if the ST rationale shows that meeting FPT_ITI.1.2 is sufficient to maintain secure operation.] The ST rationale shall provide a basic justification, showing that the first ST assignment is complete and that the metric, or metrics, called out in the second assignment are sufficient. It is acceptable to protect all data, rather than selecting specific data elements.

FPT_ITI.1.2-CSPP The TSF shall support the capability to verify the integrity of [***extension:*** security state information that is critical to maintaining a secure state among distributed systems as identified in *[**ST assignment:** list of TSF data requiring such protection]*] transmitted between the TSF and a remote trusted IT product and perform [**assignment:** automatic retransmission of data lacking integrity, with the capability to audit this action in a statistical manner] if modifications are detected. The ST rationale shall provide a basic justification, showing that the ST assignment is complete. It is acceptable to protect all data, rather than selecting specific data elements.

Refinement: See text in FPT_ITI.1.1-CSPP and FPT_ITI.1.2-CSPP
Extension: See text in FPT_ITI.1.1-CSPP and FPT_ITI.1.2-CSPP

B.7.5 FPT_RCV. 2 Automated recovery

Dependencies: ADV_SPM.1, AGD_ADM.1, FPT_TST.1

FPT_RCV.2.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.2.2 For [**assignment:** those failures indicated in the following ST assignment: *[**ST assignment:** as required by PP, list of ST specific types of TSF failures]*], the TSF shall ensure the return of the TOE to a secure state using automated procedures. As the purpose here is to ensure that the choice is made explicit, the ST rationale does not need to justify completeness, but does need to provide a basic justification for the claim that the ST will automatically recover from the failure types listed.

Refinement: See text in FPT_RCV.2.2

B.7.6 FPT_RPL.1-CSPP Replay detection

Dependencies: None

FPT_RPL.1.1-CSPP The TSF shall detect replay for the following entities [**extension:** security state information that is critical to maintaining a secure state among distributed systems as identified in *[**ST assignment:** list of TSF data requiring such protection]*]. The ST rationale shall provide a basic justification, showing that the ST assignment is complete. It is acceptable to protect all communications, rather than selecting specific entities.

FPT_RPL.1.2 The TSF shall perform [**assignment:** the action of discarding duplicates and providing the capability to audit this action in a statistical manner] when replay is detected.

Refinement: See text in FPT_RPL.1.1-CSPP
Extension: See text in FPT_RPL.1.1-CS

B.7.7 FPT_RVM.1 Non-bypassability of the TSP

Dependencies: None

FPT_RVM.1.1 The TSF shall ensure, to at least a level of confidence appropriate for a lower-level of assurance (i.e., EAL-CSPP), that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Refinement: See text in FPT_RVM.1.1

B.7.8 FPT_SEP.1 TSF domain separation

Dependencies: None

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects, at least to the extent such protection can be reasonably expected from a lower-level of assurance (i.e., EAL-CSPP), it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Refinement: See text in FPT_SEP.1.1

B.7.9 FPT_TDC.1 Inter-TSF basic TSF data consistency

Dependencies: None

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [**assignment:** information critical to security in maintaining a consistent state representation across distributed systems as identified in *[**ST assignment:** list of TSF data types]* when shared between the TSF and another trusted IT product. The ST rationale shall provide a basic justification, showing that the ST assignment is complete. It is acceptable to provide a broader definition, rather than selecting only a subset - provided the rationale shows that the security critical elements are indeed a subset of those chosen.

FPT_TDC.1.2 The TSF shall use [**assignment:** the following interpretation rules: *[**ST assignment:** list of interpretation rules to be applied by the TSF]* when interpreting the TSF data from another trusted IT product. The ST rationale shall provide a basic justification, showing that the list of rules is comprehensive and internally self-consistent.

Refinement - See text in FPT_TDC.1.1, FPT_TDC.1.2, and this added element (clarifying intent):

> FPT_TDC.1.3-CSPP The TSF shall support maintaining consistent data between this TSF and another trusted IT product for the data items specified in FPT_TDC.1.1 in accordance with the rules specified in FPT_TDC.1.2.

B.7.10 FPT_TST.1 TSF testing

Dependencies: FPT_AMT.1

FPT_TST.1.1 The TSF shall run a suite of self tests [**selection:** during initial start-up and at the request of explicitly authorized security administrator(s) or security administrator role(s)] [**assignment:** "null"] to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

Refinement: See text in FPT_TST.1.1

B.7.11 FPT_SYN-CSPP.1 TSF synchronization

Non-CC component defined in [CSPP]

Extension:

Not hierarchical to any other component.

Dependencies: None

FPT_SYN-CSPP.1.1 The TSF shall support the system capability to provide the capability to synchronize distributed TSF elements and to associate audit event records produced by multiple TSF entities.

Refinement (to CSPP component): See FPT_SYN-CSPP.1.1 in [CSPP].

Application note: This component is similar to FPT_STM "Time stamps", but calls out the synchronization requirement instead of a specifying a mechanism (i.e., reliable time stamps") that could be used for that purpose.

B.8 RESOURCE UTILIZATION (FRU)

B.8.1 FRU_RSA.1-CSPP Maximum quotas

Dependencies: None

FRU_RSA.1.1-CSPP The TSF shall enforce maximum quotas of the following resources: [**assignment:** all OS-controlled, multi-user or multi-process resources such as memory, disk space, and inter-processor communications paths] that *[**ST selection:** an individual user, a defined group of users, subjects]* can use *[**ST selection:** simultaneously, over a specified period of time]*. The ST rationale must show that the list of resources for which maximum quotas is enforced is sufficiently complete to accomplish protection against resource exhaustion, to the extent that the OS is capable of doing so. Also the ST rationale must give, for both ST selections, the reasoning for the choices made and stating why the choices support the goal of protecting against denial-of-service.

Refinement: See text in FRU_RSA.1.1-CSPP

B.9 TOE ACCESS (FTA)

B.9.1 FTA_LSA.1 Limitation on scope of selectable attributes

Dependencies: None

FTA_LSA.1.1 The TSF shall provide the capability to restrict the scope of these session security attributes: [**assignment:** user role, specific user capabilities, and any *[**ST assignment:** ST specific session security attributes]*], based on [**assignment:** user identity, point of entry, time of day, day of week, and any *[**ST assignment:** attributes specific to the ST design]*]. The ST rationale shall provide a basic justification, showing that the ST specific assignments are sufficient to restrict the security critical attributes.

Refinement: See text in FTA_LSA.1.1

B.9.2 FTA_MCS.1-CSPP Basic limitation on multiple concurrent sessions

Dependencies: FIA_UID.1

FTA_MCS.1.1-CSPP The TSF shall [**extension:** enable an authorized user to specify whether or not to] restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 If the TOE is to restrict the maximum number of concurrent sessions, the TSF shall enforce [**assignment:** an authorized user selected maximum number of] sessions per user.

Refinement: See text in FTA_MCS.1.2
Extension: See text in FTA_MCS.1.1-CSPP

B.9.3 FTA_SSL.1 TSF initiated session locking

Dependencies: FIA_UAU.1

FTA_SSL.1.1 The TSF shall lock an interactive session after [**assignment:** an authorized user specified time interval of user inactivity] by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL1.2 The TSF shall require the following events to occur prior to unlocking the session: [**assignment:** user authentication].

B.9.4 FTA_SSL.2 User-initiated locking

Dependencies: FIA_UAU.1

FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive sessions by:

a) clearing or over-writing display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other then unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [**assignment:** user authentication].

B.9.5 FTA_SSL.3 TSF-initiated termination

Dependencies: None

FTA_SSL.3.1 The TSF shall terminate an interactive session after [**assignment:** an authorized user specified time interval of user inactivity].

B.9.6 FTA_TAB.1-CSPP Default TOE access banners

Dependencies: None

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

Extension:

> FTA_TAB.1-CSPP.2 The TSF shall provide the capability for an authorized user to specify and subsequently modify the contents of this warning message.

B.9.7 FTA_TAH.1 TOE access history

Dependencies: None

FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the [**selection:** date, time, method, <u>and</u> location] of the last successful session establishment to the user.

FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the [**selection:** date, time, method, <u>and</u> location] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

Refinement: See text in FTA_TAH.1.1 and FTA_TAH.1.2

B.9.8 FTA_TSE.1 TOE session establishment

Dependencies: None

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [**assignment:** attributes that can be set by explicitly authorized security administrator(s) or security administrator role(s), including user identity, port of entry, time of day, day of the week, and any ***[ST assignment:** ST specific attributes]*. <u>The ST rationale must show that the ST assignment is complete.</u>

Refinement: See text in FTA_TSE.1.1

B.10 TRUSTED PATH/CHANNELS (FTP)

B.10.1 FTP_ITC.1-CSPP Inter-TSF trusted channel

Dependencies: None

FTP_ITC.1.1-CSPP The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the [**extension**: security information as required to mitigate against insecurities resulting from both attacks and unintentional modification, to include the following: *[**ST assignment:** other security information identified in the ST design and development]*] channel data from modification and [**extension**: identification and authentication data and the following other security information: *[**ST assignment:** other security information identified in the ST design and development*] channel data from disclosure. The ST rationale shall provide a basic justification, showing that the ST assignments are complete, with regard to mitigation in the intended operational environment for the TOE.

FTP_ITC.1.2 The TSF shall permit *[**ST selection:** the TSF, the remote trusted IT product]* to initiate communication via the trusted channel. The ST rationale shall provide a basic justification, showing that the ST selection is appropriate for maintaining secure operation in the intended environment.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**assignment:** the following functions: *[**ST assignment:** list of functions for which a trusted channel is required]*]. The ST rationale shall provide a basic justification, showing that the ST assignment is a complete list, as required to mitigate insecurities in the intended operational environment for the TOE.

Refinement: See text in FTP_ITC.1.1-CSPP, FTP_ITC.1.2, and FTP_ITC.1.3
Extension: See text in FTP_ITC.1.1-CSPP

C. APPENDIX C: TOE ASSURANCE REQUIREMENT DETAILS

C.1 CONFIGURATION MANAGEMENT (ACM)

C.1.1 ACM_CAP.3 Authorization controls

Dependencies: CM_SCP.1, ALC_DVS.1

Developer action elements:

ACM_CAP.3.1D The developer shall provide a reference for the TOE.
ACM_CAP.3.2D The developer shall use a CM system.
ACM_CAP.3.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The TOE shall be labeled with its reference.
ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.4C The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.5C The CM documentation shall describe the method used to uniquely identify the TOE configuration items.
ACM_CAP.3.6C The CM system shall uniquely identify all configuration items.
ACM_CAP.3.7C The CM plan shall describe how the CM system is used.
ACM_CAP.3.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.3.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

Evaluator action elements:

ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.1.2 ACM_SCP.2 Problem tracking CM coverage

Dependencies: ACM_CAP.3

Developer action elements:

ACM_SCP.2.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:

ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.2 DELIVERY AND OPERATION (ADO)

C.2.1 ADO_DEL.1 Delivery procedures

Dependencies: None

Developer action elements:

ADO_DEL.1.1D The developer shall document the procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe the procedures which are necessary to maintain security when distributing versions of the TOE to a user site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.2.2 ADO_IGS.1 Installation, generation, and start-up procedures

Dependencies: AGD_ADM.1

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures to be used for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2E The evaluator shall confirm that the installation procedures result in a secure configuration.

C.3 DEVELOPMENT (ADV)

C.3.1 ADV_FSP.1 Informal functional specification

Dependencies: ADV_RCR.1

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2C The functional specification shall be internally consistent.
ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

C.3.2 ADV_HLD.1 Descriptive high-level design

Dependencies: ADV_FSP.1, ADV_RCR.1

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.
ADV_HLD.1.2C The high-level design shall be internally consistent.
ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.1.6C The high-level design shall identify the interfaces of the subsystems of the TSF.
ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate an complete instantiation of the TOE security functional requirements.

C.3.3 ADV_RCR.1 Informal Correspondence Demonstration

Dependencies: None

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.3.4 ADV_SPM.1 Informal TOE security policy model

Dependencies: ADV_FSP.1

Developer action elements:

ADV_SPM.1.1D The developer shall provide an TSP model.
ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C The TSP model shall be informal.
ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.
ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.
ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that there are no security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.4 GUIDANCE DOCUMENTS (AGD)

C.4.1 AGD_ADM.1 Administrator guidance

Dependencies: ADV_FSP.1

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all security parameters under the control of the administrator indicating safe values as appropriate.

AGD_ADM.1.5C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.6C The administrator guidance shall be consistent with all other documents supplied for evaluation.

AGD_ADM.1.7C The administrator guidance shall describe all security requirements on the IT environment which are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.4.2 AGD_USR.1 User Guidance

Dependencies: ADV_FSP.1

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including all assumptions about user behavior found in the statement of TOE security environment.
AGD_USR.1.5C The user guidance shall be consistent with all other documentation delivered for evaluation.
AGD_USR.1.6C The user guidance shall describe all security requirements on the IT environment which are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.5 LIFE CYCLE SUPPORT (ALC)

C.5.1 ALC_DVS.1 Identification of security measures

Dependencies: None

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2E The evaluator shall check whether the security measures are being applied.

C.5.2 ALC_FLR.2 Flaw reporting procedures

Dependencies: None

Developer action elements:

ALC_FLR.2.1D The developer shall document the flaw remediation procedures.
ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon user reports of security flaws and requests for corrections to those flaws.

Content and presentation of evidence elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.2.5C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.
ALC_FLR.2.6C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

Evaluator Action Elements:

ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.6 TESTS (ATE)

C.6.1 ATE_COV.2 – Analysis of coverage

Dependencies: ADV_FSP.1, ATE_FUN.1

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator Actions:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.6.2 ATE_DPT.1 Testing: High Level Design

Dependencies: ADV_HLD.1, ATE_FUN.1

Developer action elements:

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.2.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TOE operates in accordance with the high level design.

Evaluator action elements:

ATE_DPT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.6.3 ATE_FUN.1 Functional Testing

Dependencies: None

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.
ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C The test results in the test documentation shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each security function operates as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C.6.4 ATE_IND.2 Independent Testing - Sample

Dependencies: ADV_FSP.1, AGD_USR.1, AGD_ADM.1, ATE_FUN.1

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E The evaluator shall test the TSF to confirm that the TSF operates as specified.
ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

C.7 VULNERABILITY ASSESSMENT (AVA)

C.7.1 AVA_MSU.2 Validation of Analysis

Dependencies: ADO_IGS.1, AGD_ADM.1, AGD_USR.1, ADV_FSP.1

Developer action elements:

AVA_MSU.2.1D The developer shall provide guidance documentation.
AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE, including operation following failure or operational error, their consequences and implications for maintaining secure operation.
AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.2.3.C The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.2.5C The developer's analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to check that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.
AVA_MSU.2.4E The evaluator shall confirm that the analysis shows that guidance is provided for secure operation in all modes of operation of the TOE.

C.7.2 AVA_SOF.1 Strength of TOE Security Function Evaluation

Dependencies: ADV_FSP.1, ADV_HLD.1

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each identified mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

C.7.3 AVA_VLA.1 Developer vulnerability analysis

Dependencies: ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

Developer action elements:

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2D The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.1.1C The evidence shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2E The evaluator shall conduct penetration testing, based on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

C.8 MAINTENANCE OF ASSURANCE (AMA)

None

D. APPENDIX D: IT-ENVIRONMENT FUNCTIONAL REQUIREMENT DETAILS

This section contains information on the security functional requirements expected of the hardware/firmware platform upon which the CSPP-OS compliant TOE is to be run. By identifying these requirements, it becomes possible to specify OS requirements separate from underlying platform requirements. This in turn enables the composition of a compliant OS with any number of underlying platforms and being able to make definitive (to the level of confidence appropriate for EAL-CSPP) claims about the security provided by the OS/platform pair.

Throughout these requirements the term “BIOS” (basic input-output system), while a PC specific term, is used in its most general sense to mean “any underlying hardware/firmware input/output support used by the operating system or capable of by-passing operating system protections”. An example of the latter would be a “BIOS” which provided buffering of read/writes to disk through a BIOS “owned” portion of memory. Any residual information protection for this shared resource must be performed by the BIOS as the operating system is unable to do so.

D.1 AUDIT (FAU)

D.1.1 FAU_STG.1 Protected audit trail storage

Dependencies: FAU_GEN.1-CSPP

FAU_STG.1.1 The TSF’s IT-environment shall help protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF’s IT-environment shall be able to [**selection:** prevent] modifications to the audit records via hardware write protection to removable storage media.

D.2 USER DATA PROTECTION (FDP)

D.2.1 FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1-CSPP

FDP_ACC.1.1 The TSF’s IT-environment shall enforce the [**assignment:** requirement to provide a ‘boot-level’ password, if so required based upon a user-selectable parameter,] on [**assignment:** the ability to boot or re-boot the system].

D.2.2 FDP_RIP.1 Subset residual information protection

Dependencies: None

FDP_RIP.1.1 The TSF’s IT-environment shall ensure that any previous information content of a resource is made unavailable upon the [**assignment:** following ST selection: *[**ST selection:** either allocation of the resource to, deallocation of the resource from, or both]*] the following objects [**assignment:** any BIOS-controlled shared memory and file storage space].

D.3 IDENTIFICATION AND AUTHENTICATION (FIA)

D.3.1 FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1

FIA_UAU.1.1 If password-protected system bootup is enabled, the TSF’s IT-environment shall allow [**assignment:** a limited number of authentication attempts] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 If password-protected system bootup is enabled, the TSF’s IT-environment shall require each user to be successfully authenticated before allowing any other TSF’s IT-environment-mediated actions on behalf of the user.

D.3.2 FIA_UAU.6 Re -authentication

Dependencies: None

FIA_UAU.6.1 If password-protected system bootup is enabled, the TSF’s IT-environment shall re-authenticate the user under the conditions [**assignment:** of system re-boot from the operating state].

D.3.3 FIA_UAU.7 Protected authentication feedback

Dependencies: FIA_UAU.1

FIA_UAU.7.1 The TSF’s IT-environment shall not provide [**assignment:** any indication of success or failure nor clear-text display of any secret authenticator] to the user while the authentication is in progress.

D.4 SECURITY MANAGEMENT (FMT)

D.4.1 FMT_MOF.1 Management of security functions behavior

Dependencies: FMT_SMR.1

FMT_MOF.1.1 The TSF's IT-environment shall restrict the ability to [**selection:** disable or enable] the functions [**assignment:** of password-protected boot-up] to [**assignment:** directly connected keyboard entry and, if currently enabled, to only users who have been successfully authenticated].

D.4.2 FMT_MSA.3 Static attribute initialization

Dependencies: -FMT_MSA.1, FMT_SMR.1

FMT_MSA.3.1 The TSF's IT-environment shall enforce the [**assignment:** CSPP access control SFP] to provide [**assignment:** function-disabled] as the default value for password-protected system boot-up.

FMT_MSA.3.2 The TSF's IT-environment need not allow the [**assignment:** any users the capability] to specify alternate initial default value for the password-protected boot-up function.

D.4.3 FMT_MTD.1 Management of TSF's IT-environment data

Dependencies: FMT_SMR.1

FMT_MTD.1.1 The TSF's IT-environment shall restrict the ability to [**selection:** change_default, read, modify, delete, or clear] the [**assignment:** all internal TSF's IT-environment (i.e., the BIOS) data structures that are security critical] to [**assignment:** only the BIOS].

D.5 PROTECTION OF TRUSTED SECURITY (FPT)

D.5.1 FPT_AMT.1 Abstract machine testing

Dependencies: None

FPT_AMT.1.1 The TSF's IT-environment shall run a suite of tests [**selection:** during initial start-up] to demonstrate the correct operation of the security assumptions provided by the hardware which underlies the TSF's IT-environment.

D.5.2 FPT_RCV. 2 Automated recovery

Dependencies: ADV_SPM.1, AGD_ADM.1, FPT_TST.1

FPT_RCV.2.1 When automated recovery from a failure or service discontinuity is not possible, the TSF's IT-environment shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.2.2 For [**assignment:** system re-boot], the TSF's IT-environment shall ensure the return of the TOE to a secure state using automated procedures.

D.5.3 FPT_RVM.1 Non-bypassability of the TSP

Dependencies: None

FPT_RVM.1.1 The TSF's IT-environment shall ensure, to at least a level of confidence appropriate for a lower-level of assurance (i.e., EAL-CSPP), that BIOS-level, TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

D.5.4 FPT_SEP.1 TSF domain separation

Dependencies: None

FPT_SEP.1.1 The TSF's IT-environment shall maintain a security domain for its own execution that protects, at least to the extent such protection can be reasonably expected from a lower-level of assurance (i.e., EAL-CSPP), it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF's IT-environment shall enforce separation between the BIOS and hardware-level security domains and the other security domains of the OS and applications by using the hardware separation features common with today's processors.

D.5.5 FPT_SYN-CSPP.1 TSF synchronization

Non-CC component defined in [CSPP]

Extension:

Not hierarchical to any other component.

Dependencies: None

FPT_SYN-CSPP.1.1 The TSF's IT-environment shall support the system capability to provide the capability to synchronize distributed TSF's IT-environment elements and to associate audit event records produced by multiple TSF's IT-environment entities by providing a real-time clock and the necessary programmatic interfaces.

Refinement (to CSPP component): See text in FPT_SYN-CSPP.1.1

Application note: This component is similar to FPT_STM "Time stamps", but calls out the synchronization requirement instead of a specifying a mechanism (i.e., reliable time stamps") that could be used for that purpose. For the IT underlying an operating system, a real-time clock will be an important part of meeting this requirement.

D.6 RESOURCE UTILIZATION (FRU)

None.

D.7 TOE ACCESS (FTA)

D.7.1 FTA_TAH.1 TOE access history

Dependencies: None

FTA_TAH.1.1 Upon successful system boot-up, the TSF's IT-environment need not display the [**selection:** any information about] the last successful system boot-up to the user.

FTA_TAH.1.2 If password-protected system boot-up is enabled and an unsuccessful boot-up authentication attempt has occurred since the last successful attempt, then upon successful session establishment, the TSF's IT-environment shall display the [**selection:** date and time] of the last unsuccessful boot-up authentication attempt.

FTA_TAH.1.3 The TSF's IT-environment shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

D.8 TRUSTED PATH/CHANNELS (FTP)

None.